



Oeson
Inspiring generation

DHCP using HYENAE

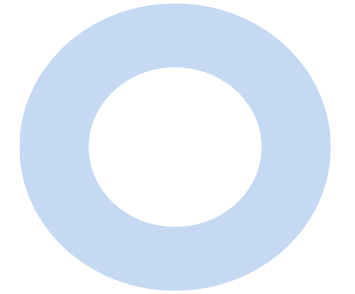


Developed By Wilson Canete Kamacupa





Agenda



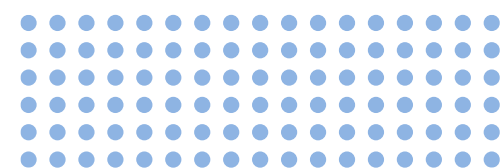
- 1 PROJECT OBJECTIVE
- 2 PROJECT REQUIREMENT
- 3 DHCP INTRODUCTION AND CONFIGURATION
- 4 INTRODUCTION OF HYENAE TOOL
- 5 INSTALLATION STEPS FOR HYENAE IN WINDOWS
- 6 DHCP ATTACK USING HYENAE
- 7 CONCLUSION
- 8 REFERENCE





Warning

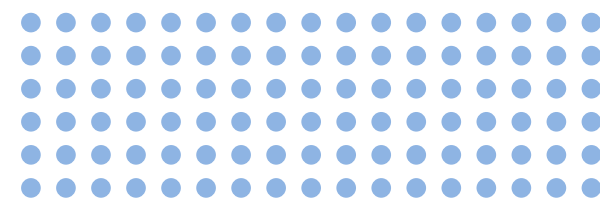
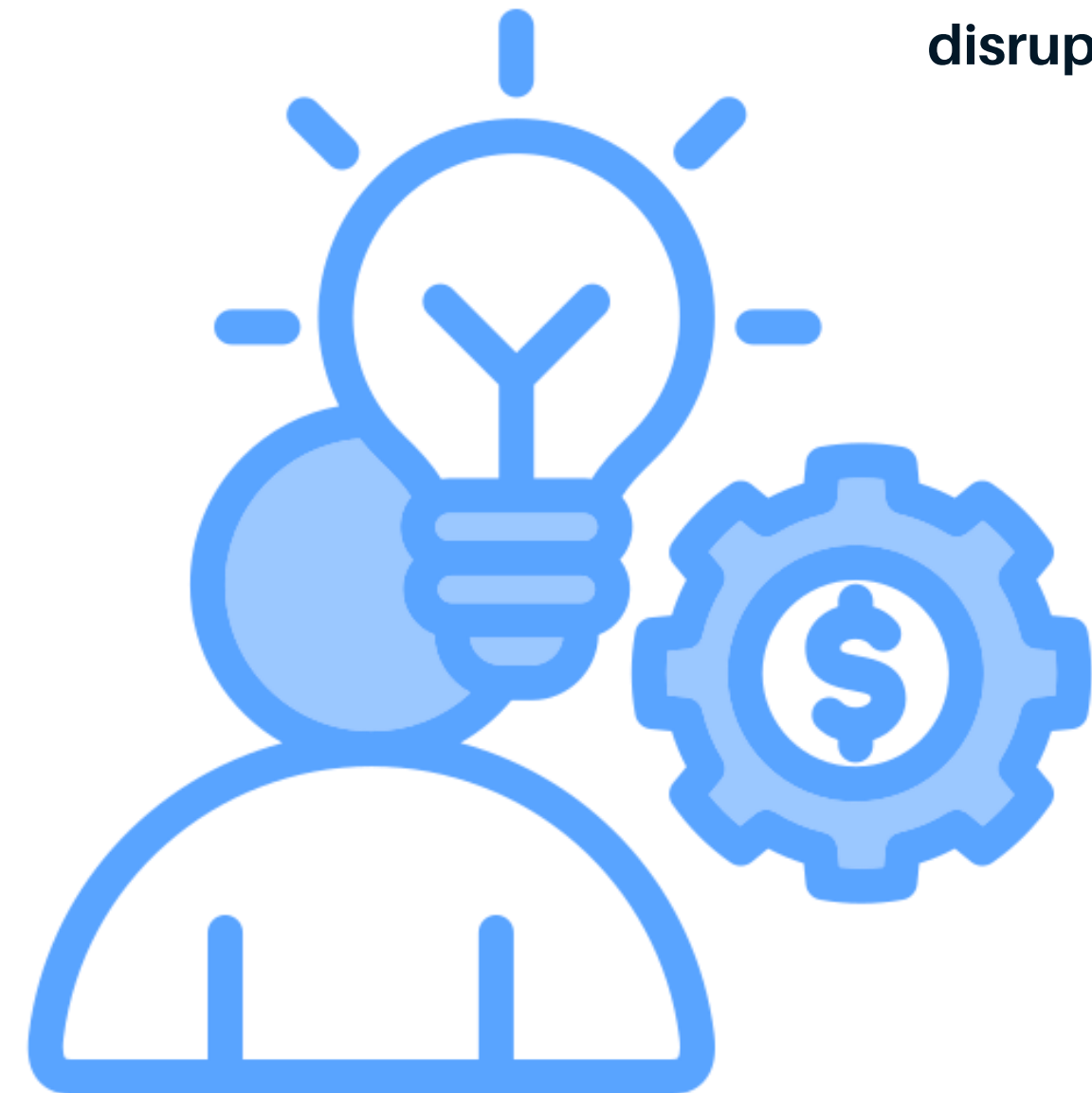
- 1 The information provided in this presentation is intended for educational purpose only.
- 2 Unauthorized scanning or exploitation of system is illegal and unethical.
- 3 Always obtain proper authorization before conducting any security assessments.

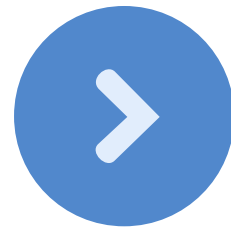




Project Objective

The objective of this project is to demonstrate a DHCP starvation attack using Hyenae tool, a network packet generator. This attack will target a Windows Server DHCP service, simulating a real-world scenario where an attacker depletes available IP addresses, disrupting network operations.





Project Requirement



Primary Host

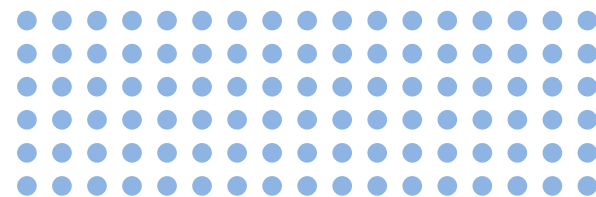
Windows 11

Virtual Machine

Windows Server configured Bridged Adapter Network

Tool

Hyenae (hyenae Advanced Network Evaluator) will be used for generating and manipulating packets on the network

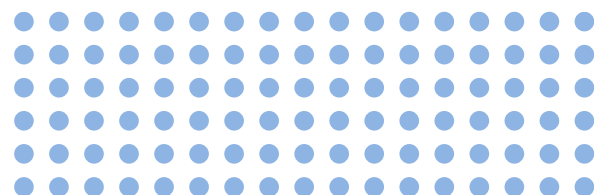




DHCP Introduction and Configuration

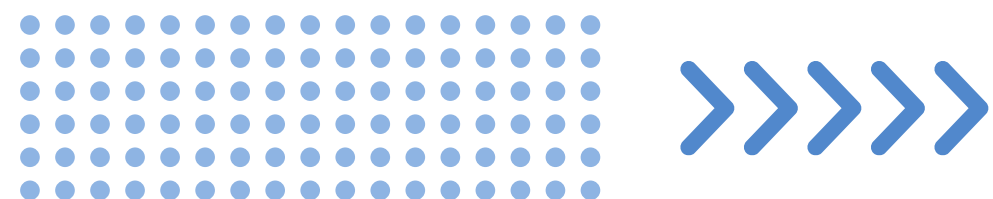
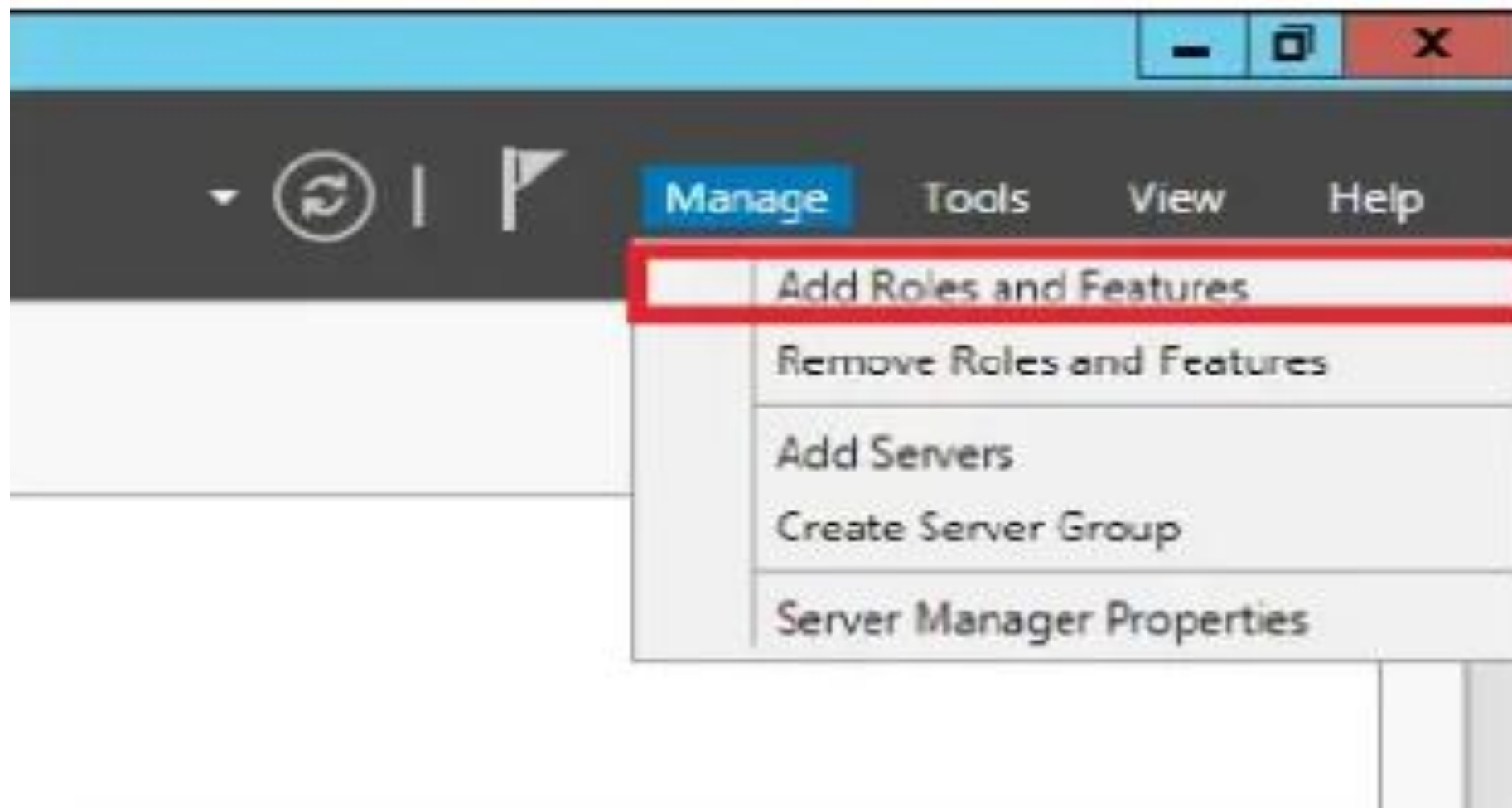
DHCP (Dynamic Host Configuration Protocol)

Is a network protocol used to automatically assign IP addresses and other configuration parameters to devices on a network. It simplifies the process of setting up and managing IP addresses by dynamically allocating them as devices connect to the network. This is especially useful in larger networks where manual IP address configuration would be time-consuming and error-prone.

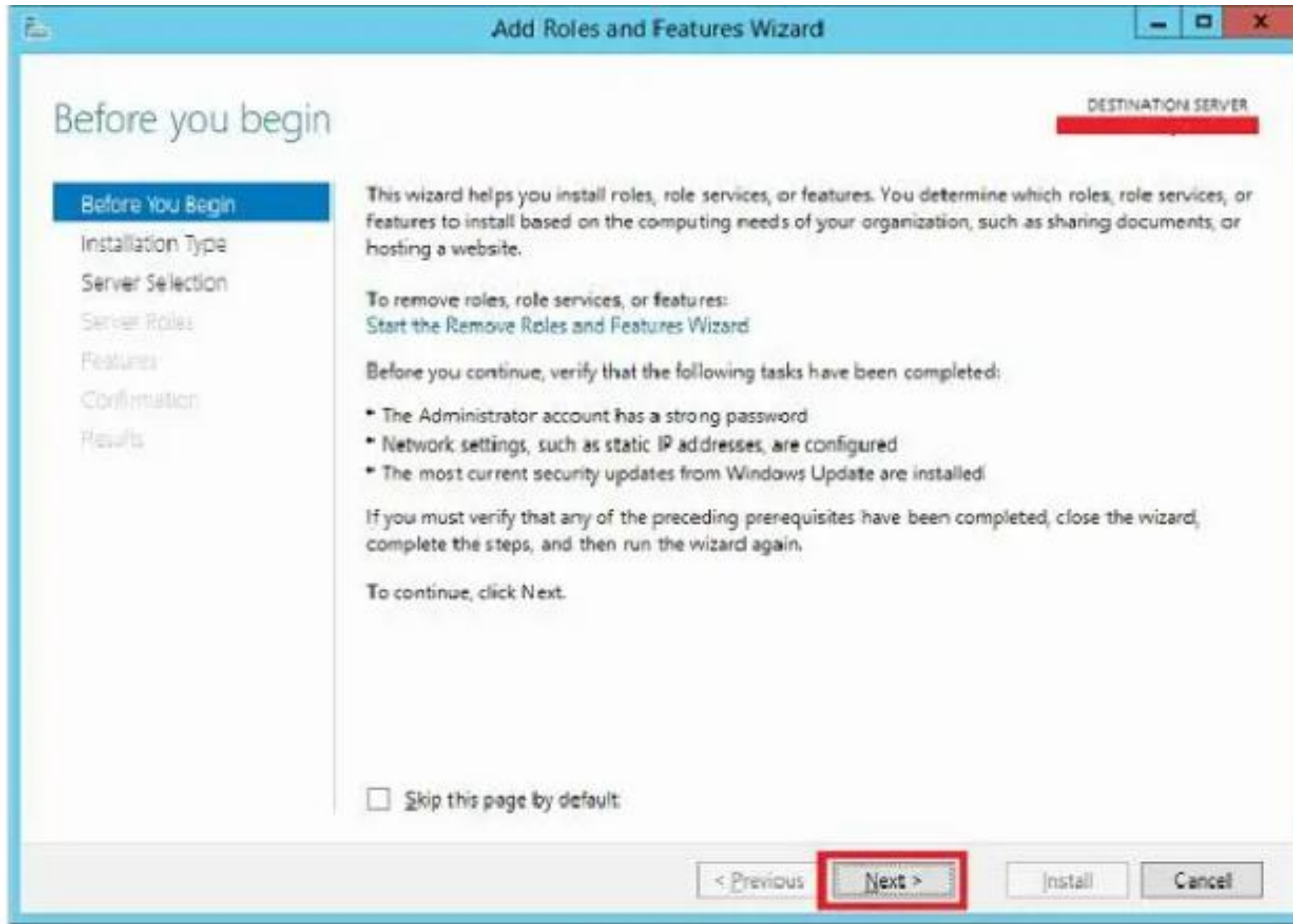


To install DHCP in Windows Server you will have to follow the steps given below

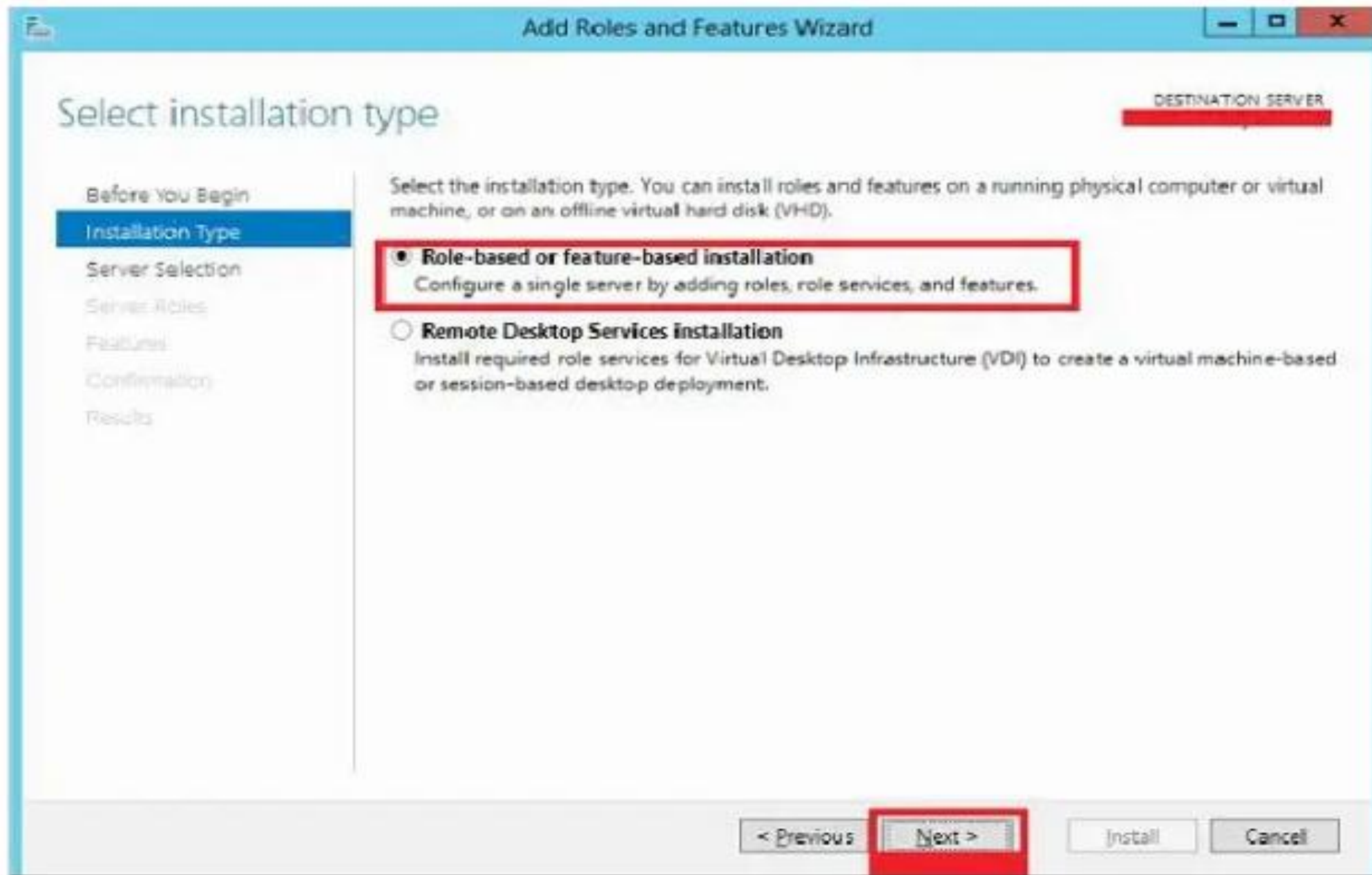
Step 1 - Go to "Server Manager" → Manager → Add Roles and Features



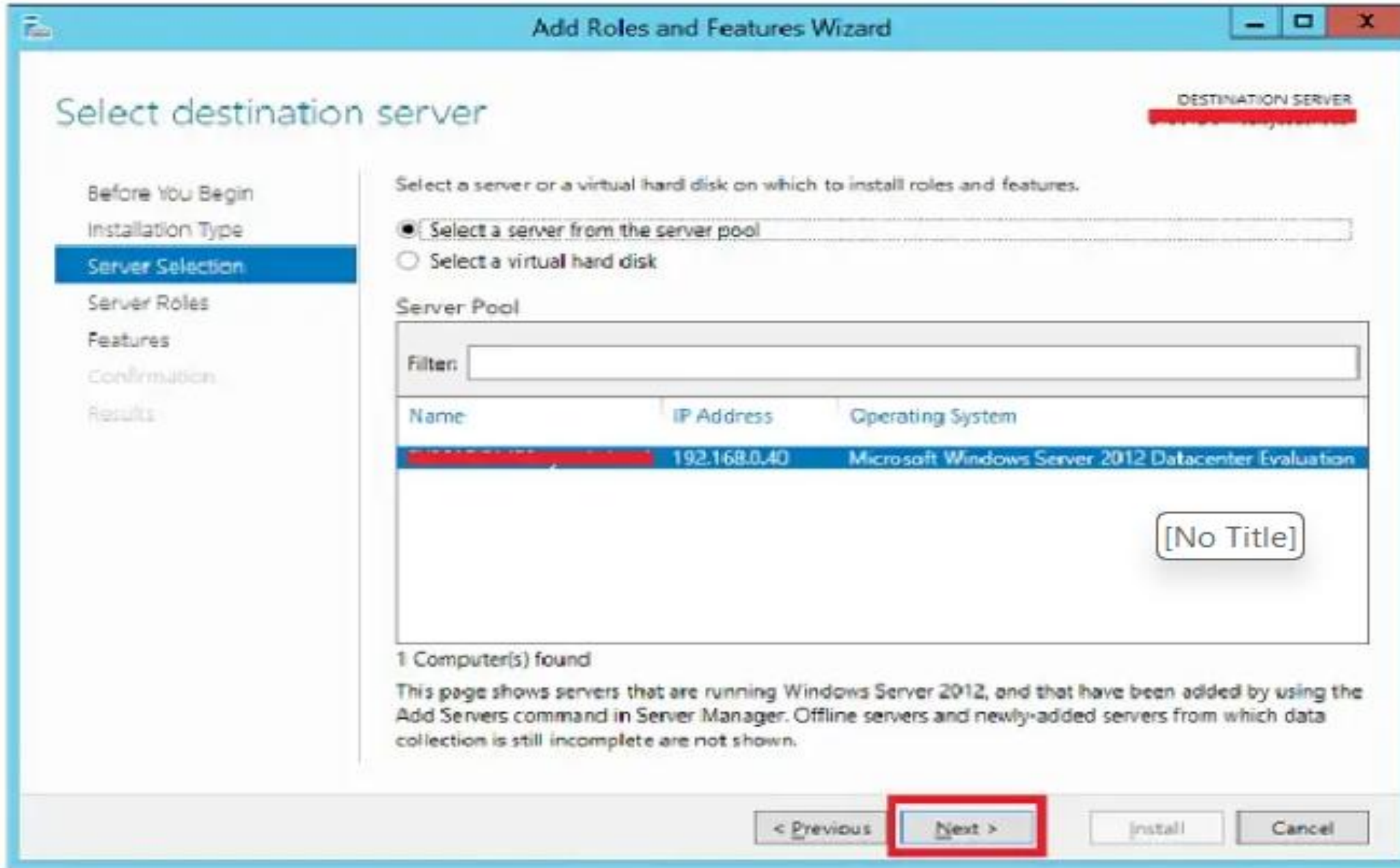
Step 2 - Click Next



Step 3 - Select the Role-based or feature-based installation option → click Next



Step 4 - We will install a Local DHCP Role as it will select a server from the Server pool → click Next



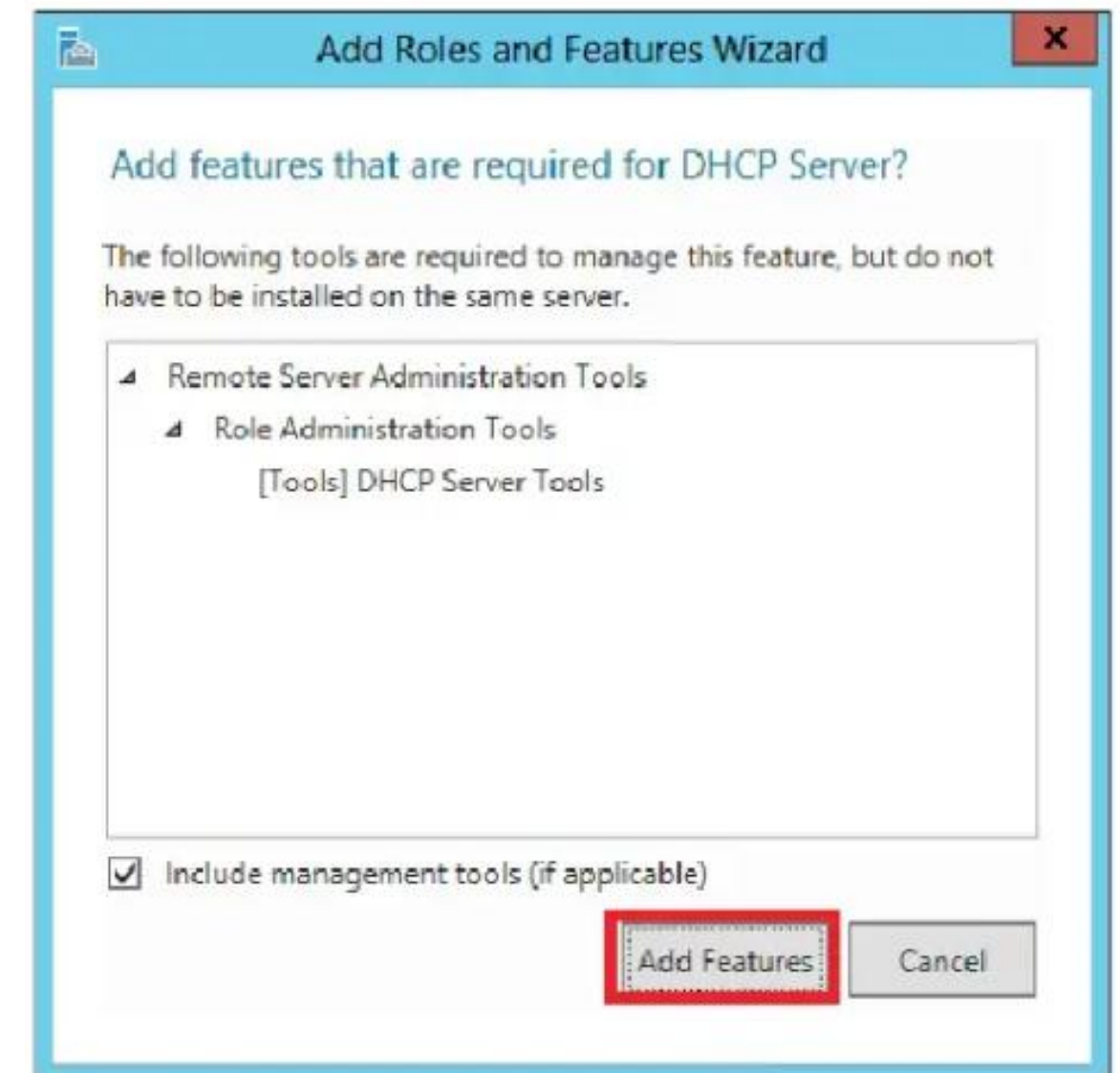
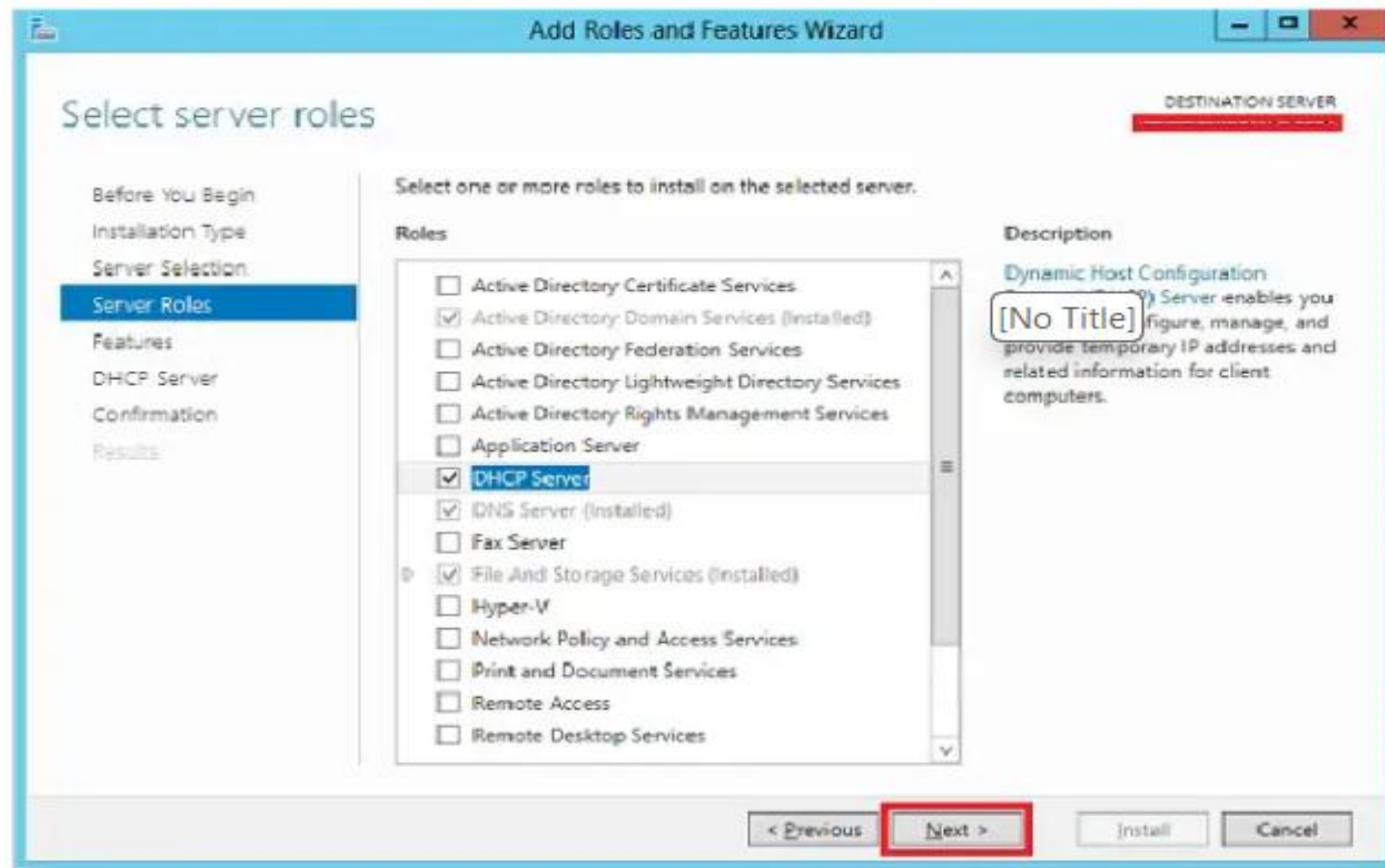
The screenshot shows the 'Add Roles and Features Wizard' window. The title bar reads 'Add Roles and Features Wizard'. The main heading is 'Select destination server'. On the left, a navigation pane lists: 'Before You Begin', 'Installation Type', 'Server Selection' (highlighted), 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main area contains the text: 'Select a server or a virtual hard disk on which to install roles and features.' Below this are two radio buttons: 'Select a server from the server pool' (selected) and 'Select a virtual hard disk'. Under the 'Server Pool' section, there is a 'Filter' text box and a table with the following data:

Name	IP Address	Operating System
192.168.0.40	192.168.0.40	Microsoft Windows Server 2012 Datacenter Evaluation

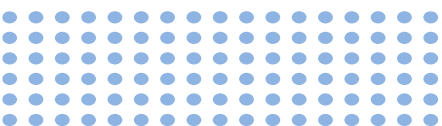
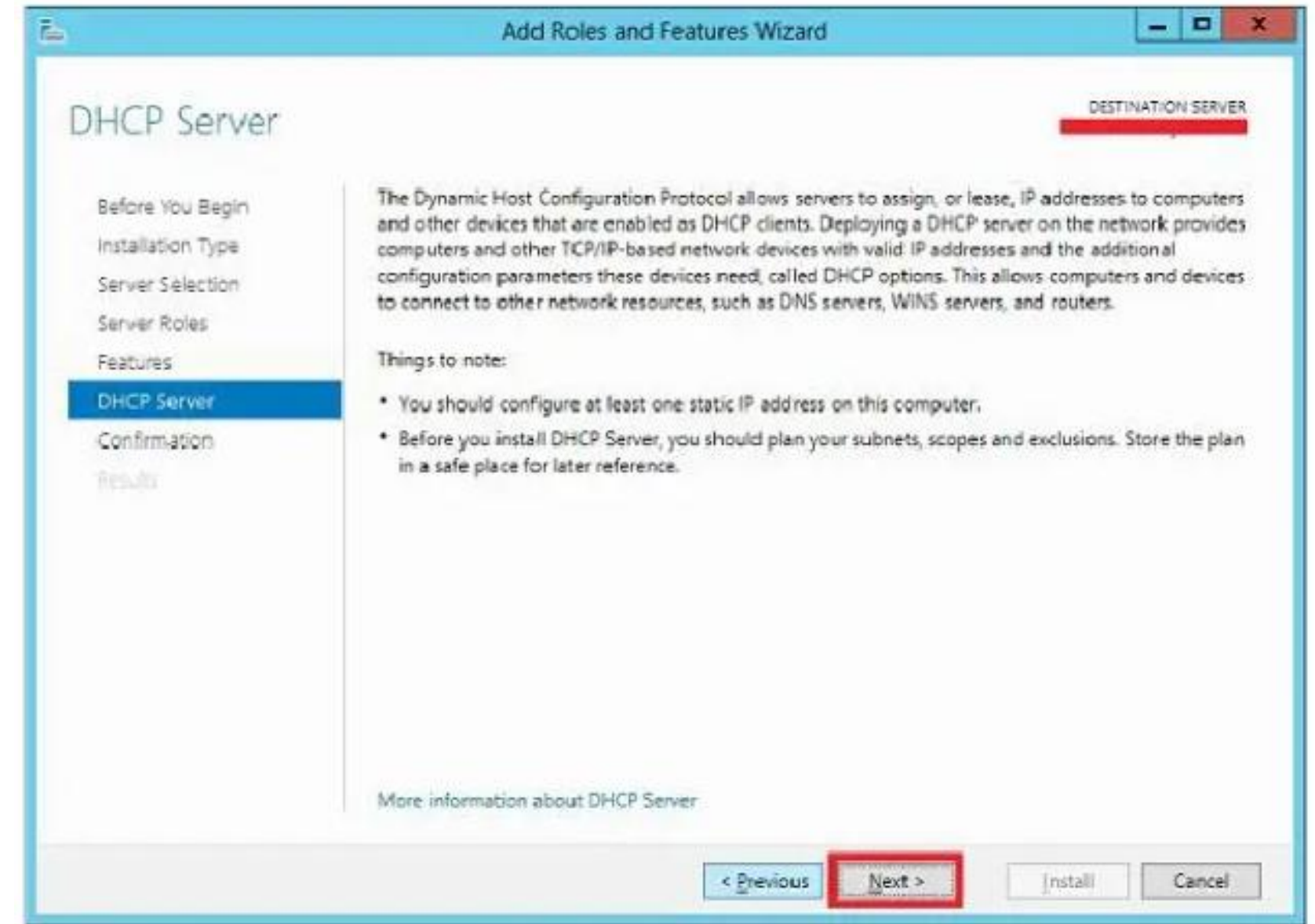
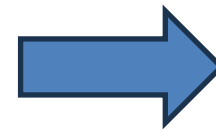
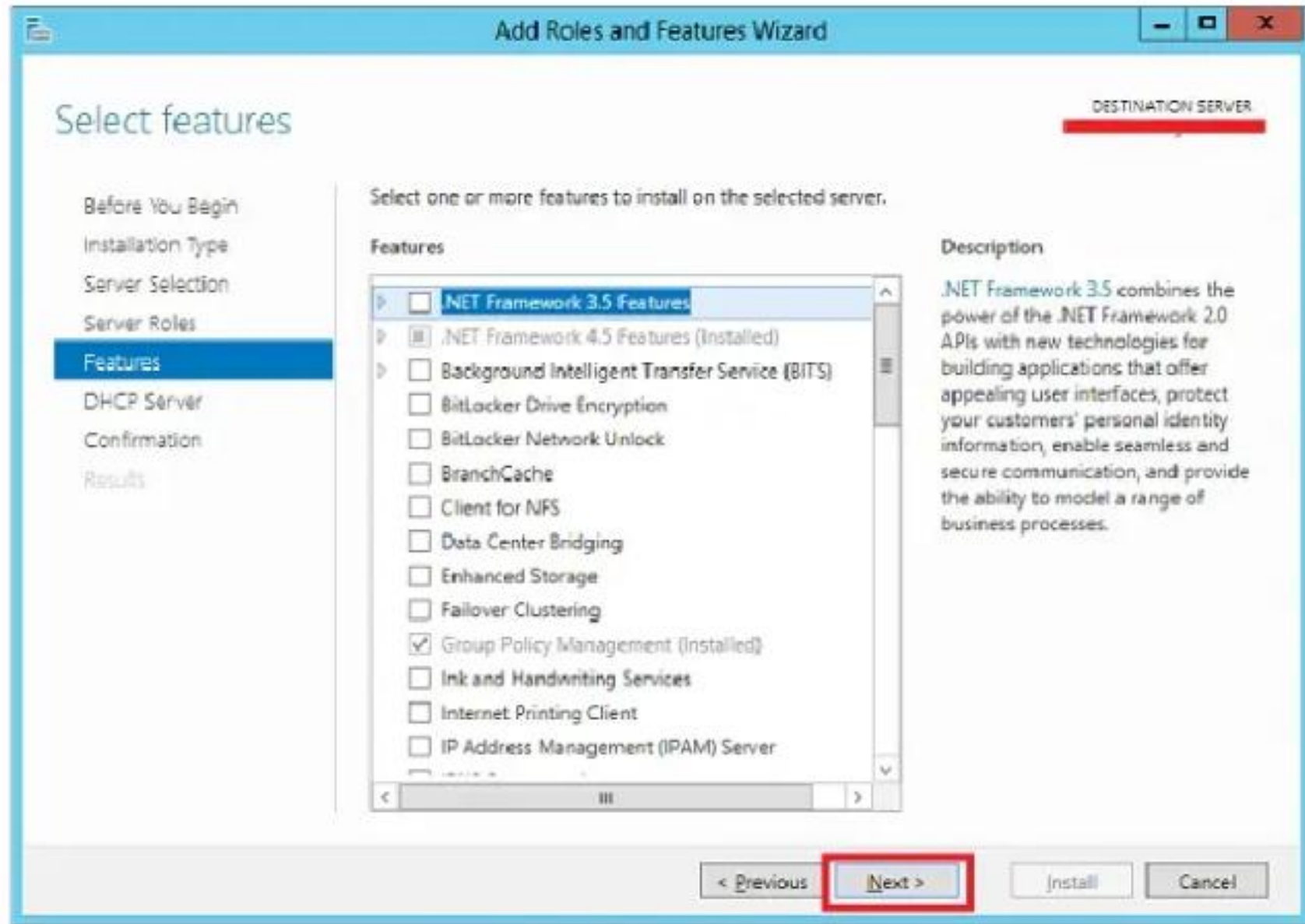
Below the table, it says '1 Computer(s) found'. A note at the bottom states: 'This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.' At the bottom right, there are four buttons: '< Previous', 'Next >' (highlighted with a red box), 'Install', and 'Cancel'. A red box also highlights the 'DESTINATION SERVER' label at the top right of the main area.



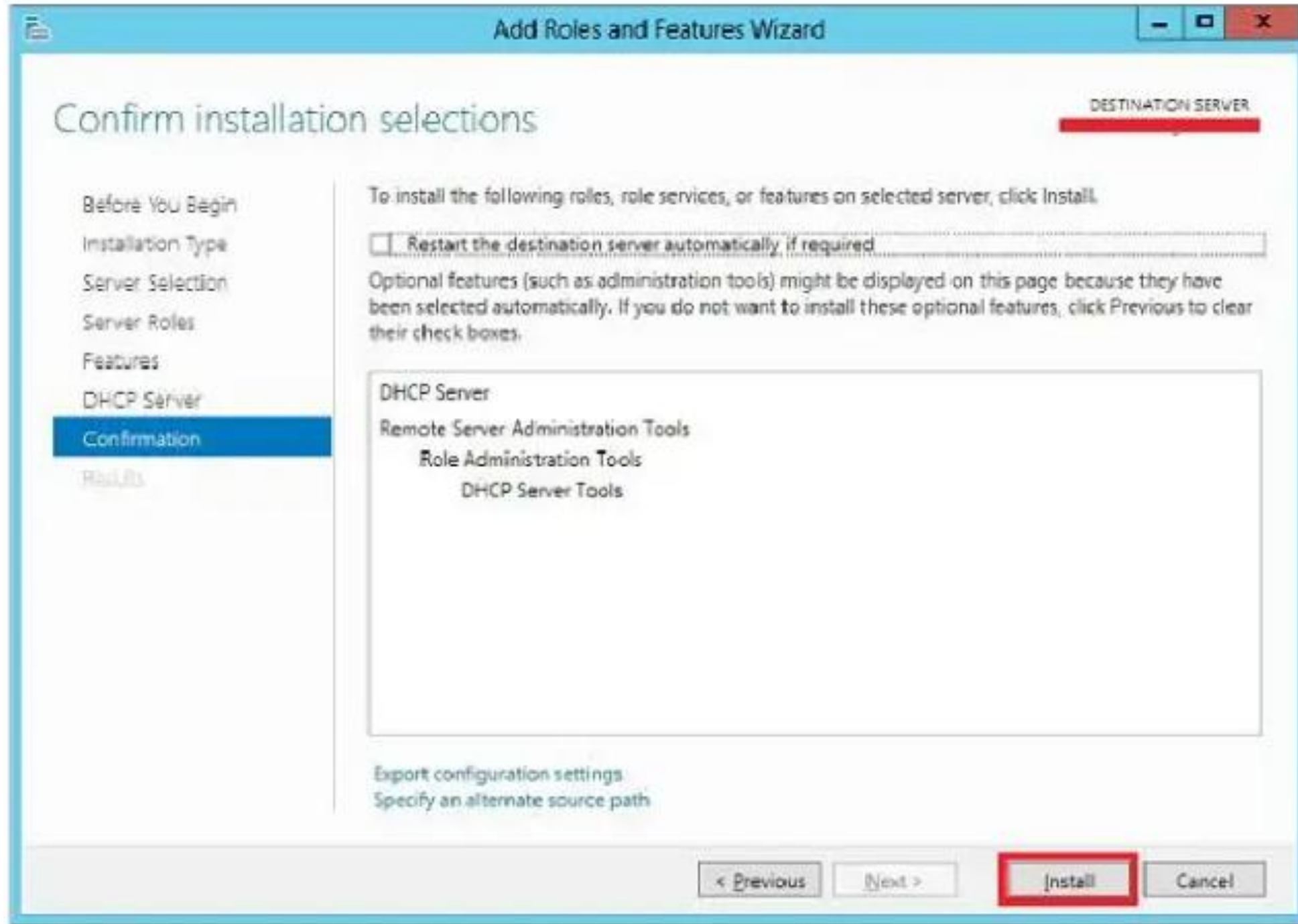
Step 5 - From the Roles lists, check the DHCP Server role → click Add Features on the popup windows as shown in the following screenshots



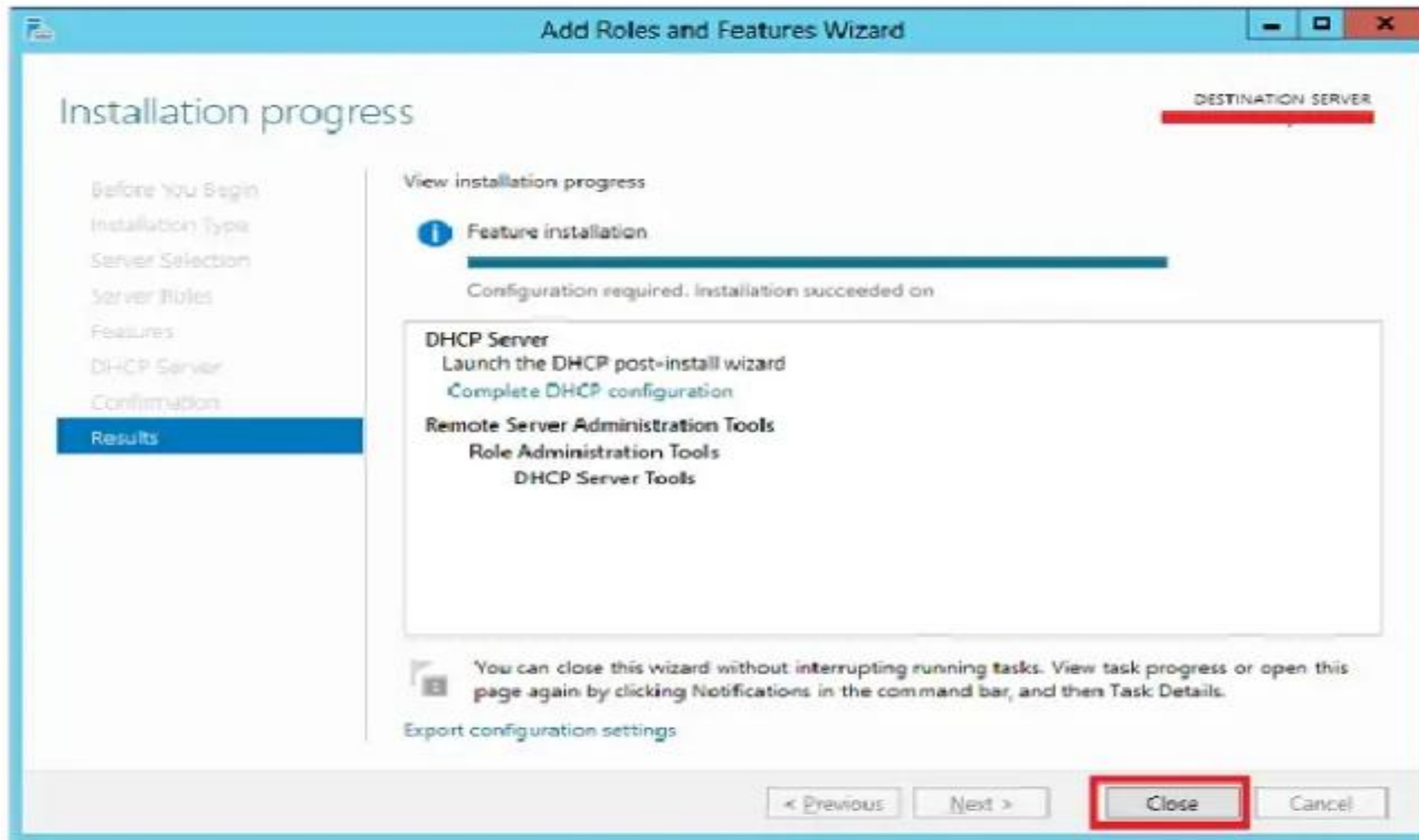
Step 6 - Click Next



Step 7 - Click Install

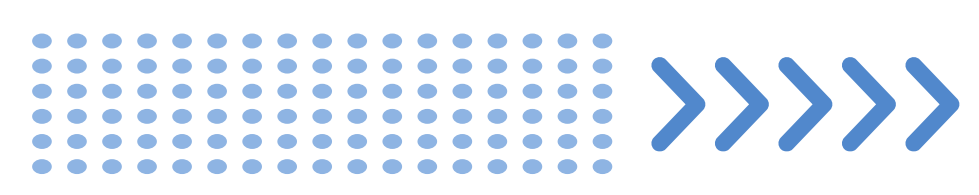
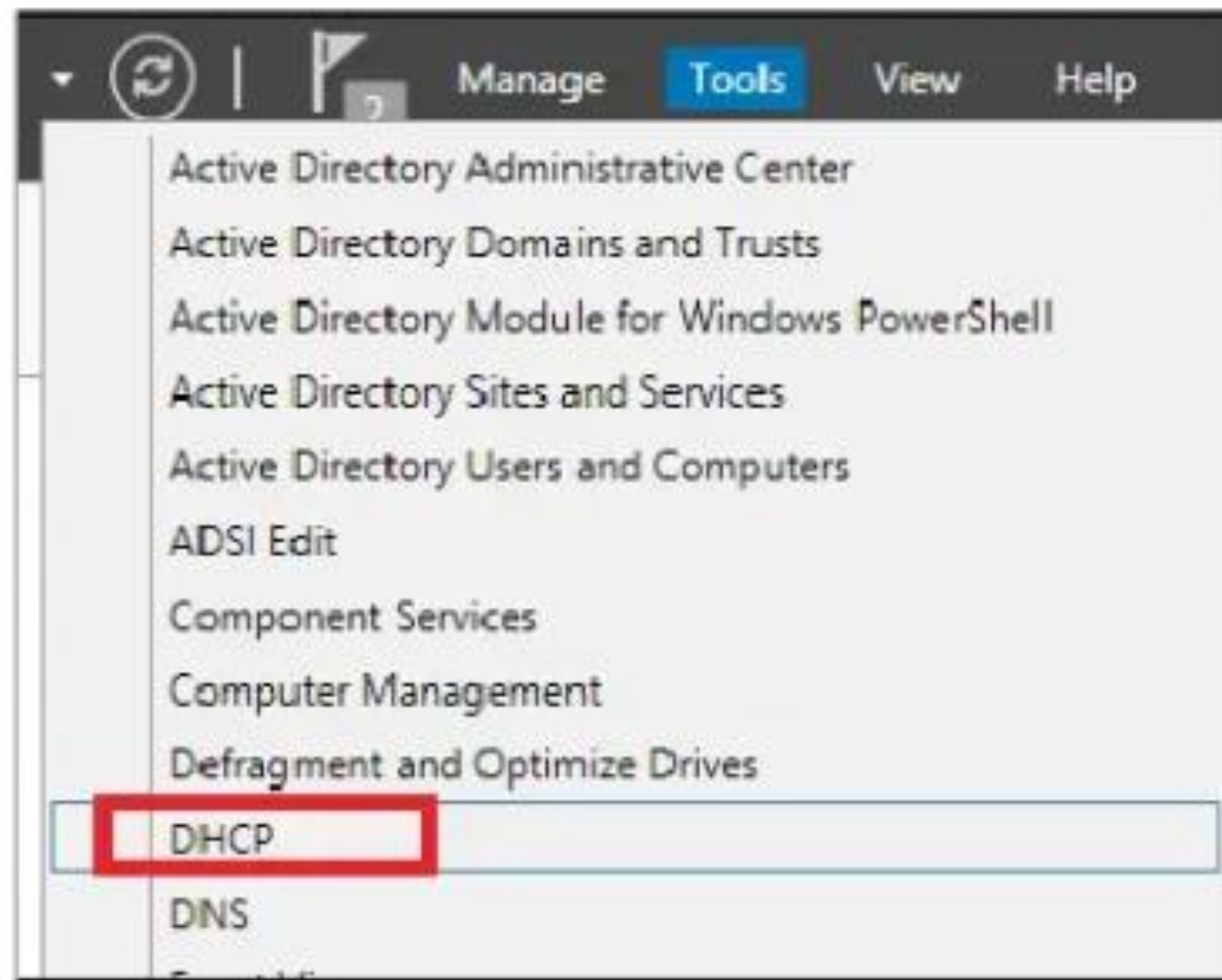


Step 8 - Click close

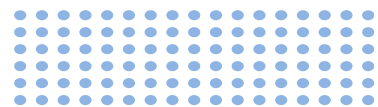
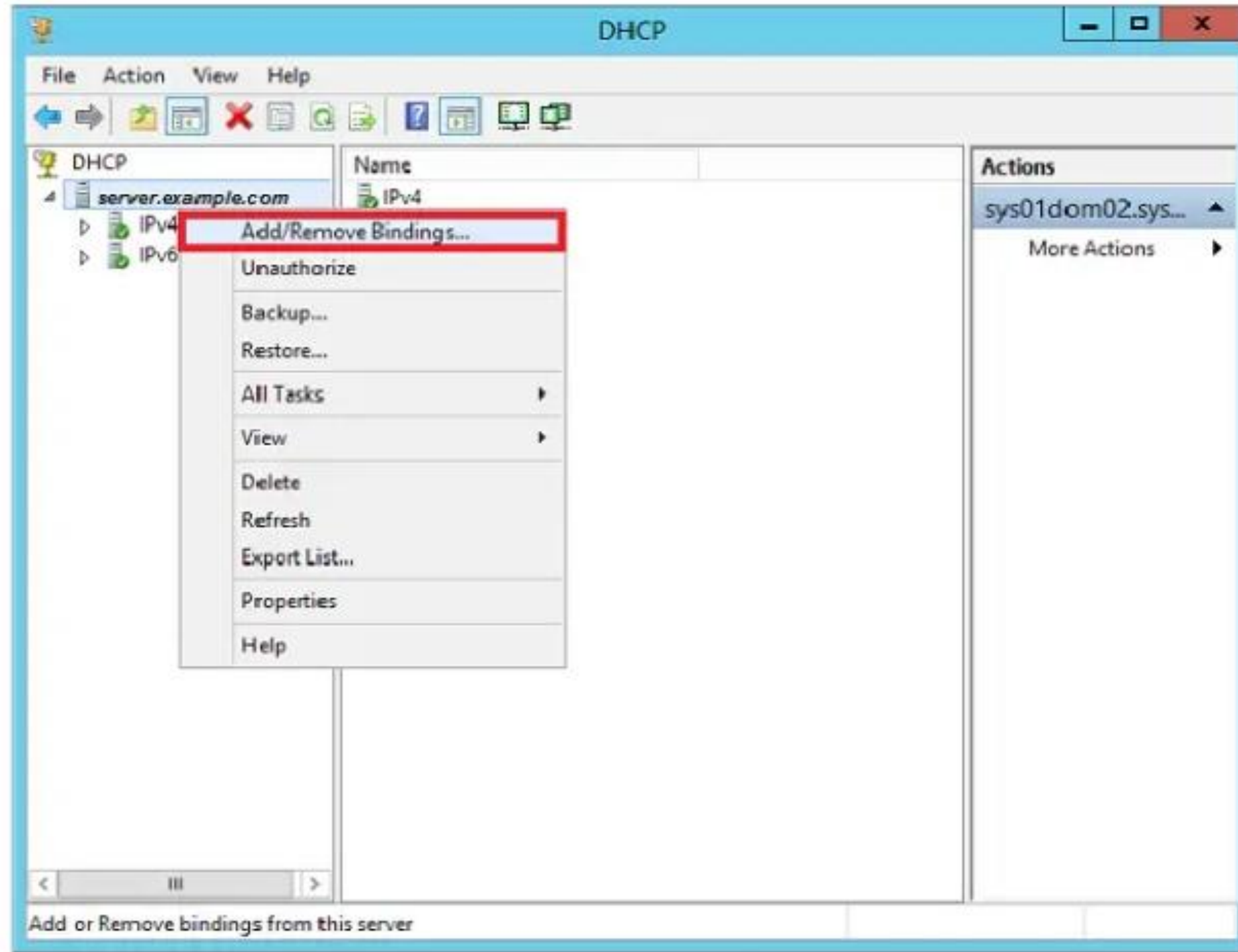


Now we have to configure the service to make it useful for the computers. To do this, we need to follow the steps given below

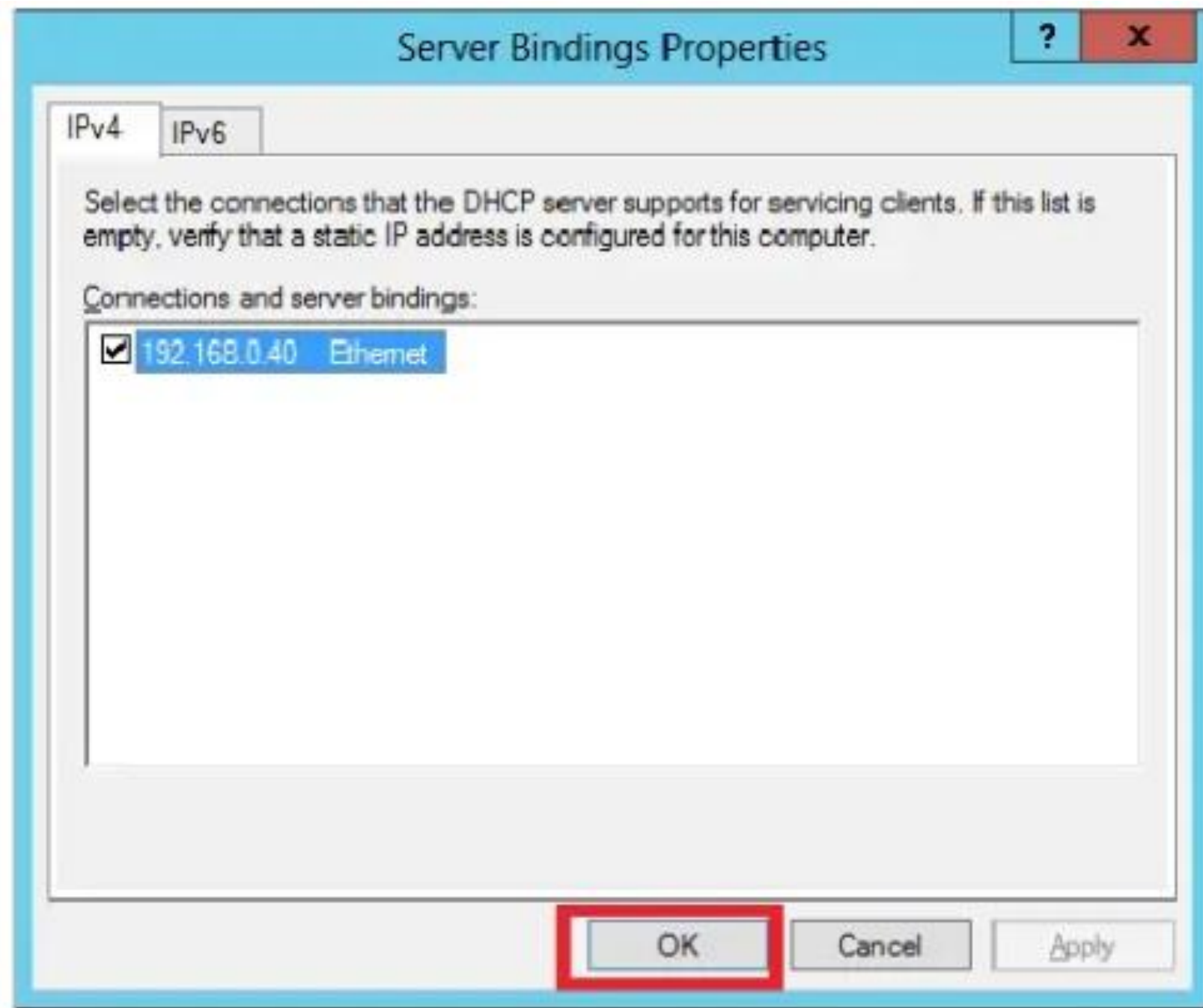
Step 1 - Server Manager screen → Tools → DHCP



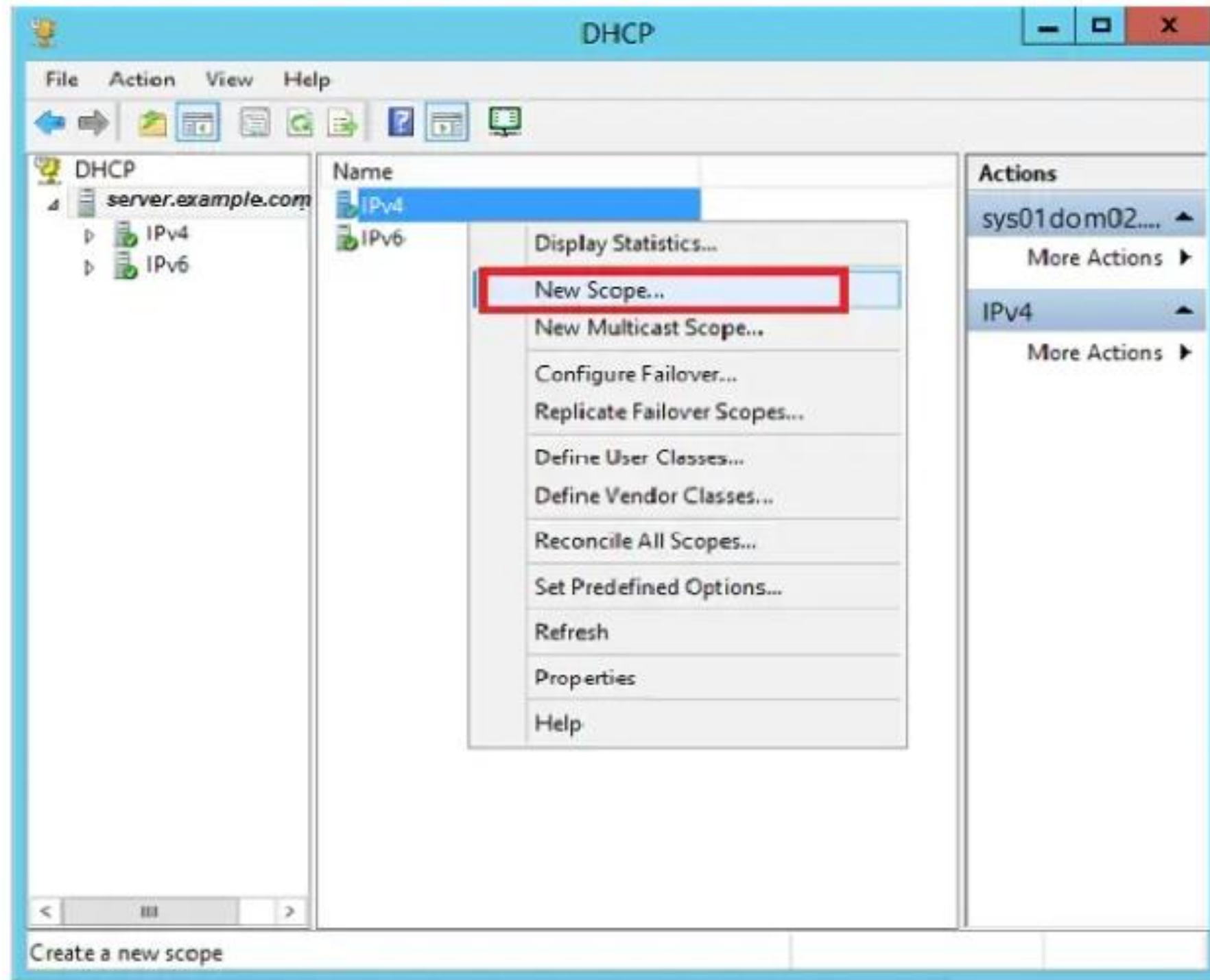
Step 2 - Right click on the DHCP Server → then click on “Add/Remove Bindins...”



Step 3 - Ensure the static IP address of the server should appear as shown in the following screenshot



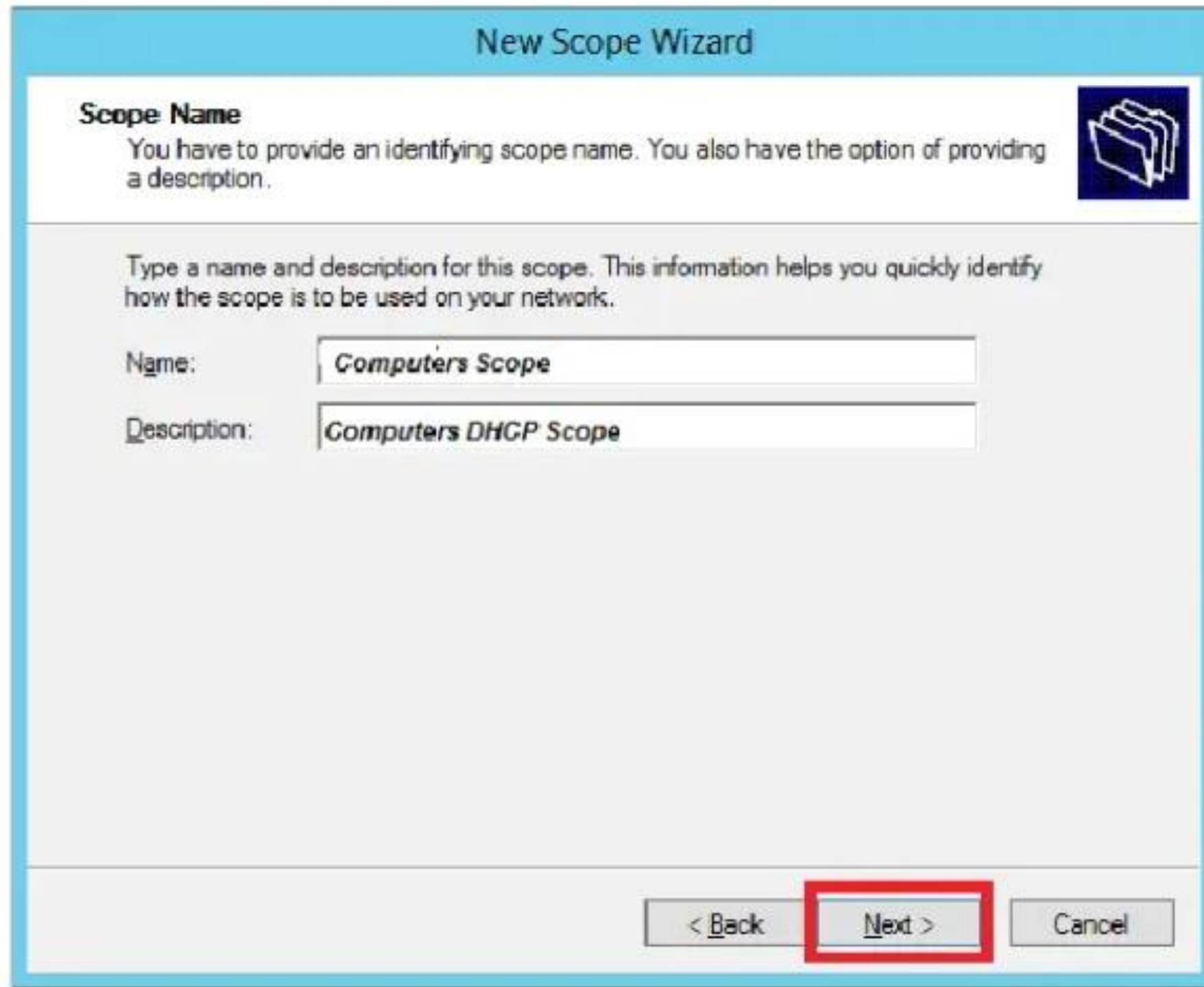
Step 4 - Right click on IPv4 → Select “New Scope”



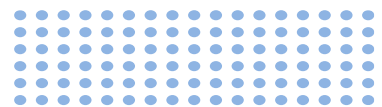
Step 5 - Click Next



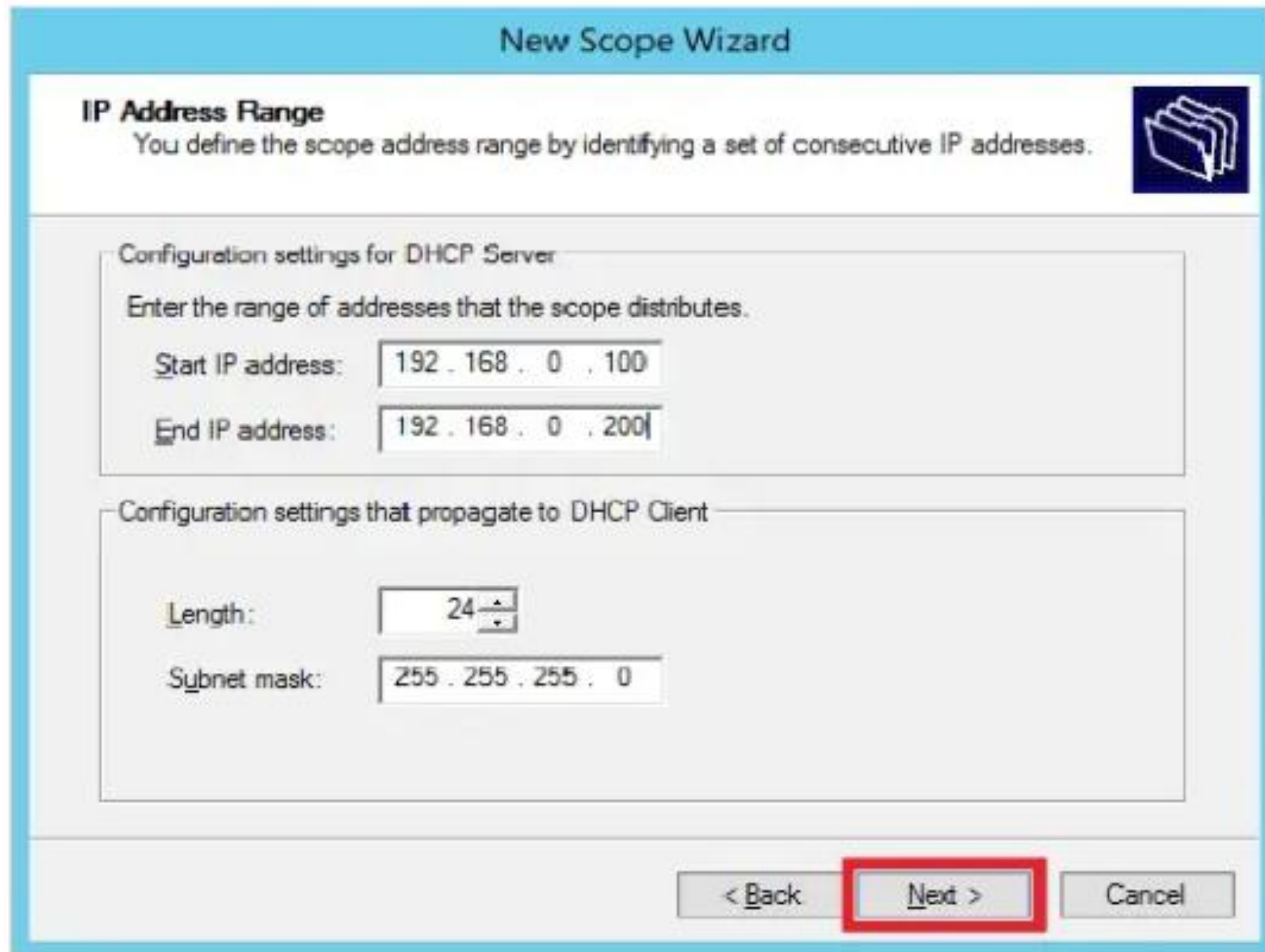
Step 6 - Enter Scope Name and Description as shown in the following screenshot and then → Next



The screenshot shows a 'New Scope Wizard' dialog box. It has a title bar with the text 'New Scope Wizard'. Below the title bar, there is a section titled 'Scope Name' with a folder icon. The text below this section says: 'You have to provide an identifying scope name. You also have the option of providing a description.' Below this, there is a larger text area with the instruction: 'Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.' There are two input fields: 'Name:' with the text 'Computers Scope' and 'Description:' with the text 'Computers DHCP Scope'. At the bottom of the dialog box, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red rectangle.



Step 7 - Enter the Start and End IP address, the Subnet mask, leave the Length as default “24” for class C subnet → click Next



The image shows a Windows 'New Scope Wizard' dialog box. The title bar is blue and says 'New Scope Wizard'. The main area has a light blue header with the text 'IP Address Range' and a sub-header 'You define the scope address range by identifying a set of consecutive IP addresses.' Below this, there are two sections. The first section is titled 'Configuration settings for DHCP Server' and contains the text 'Enter the range of addresses that the scope distributes.' It has two input fields: 'Start IP address:' with the value '192 . 168 . 0 . 100' and 'End IP address:' with the value '192 . 168 . 0 . 200'. The second section is titled 'Configuration settings that propagate to DHCP Client' and contains two input fields: 'Length:' with the value '24' and 'Subnet mask:' with the value '255 . 255 . 255 . 0'. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red rectangular border.

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

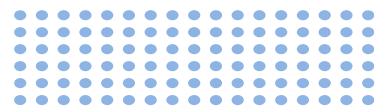
Configuration settings for DHCP Server
Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 0 . 100
End IP address: 192 . 168 . 0 . 200

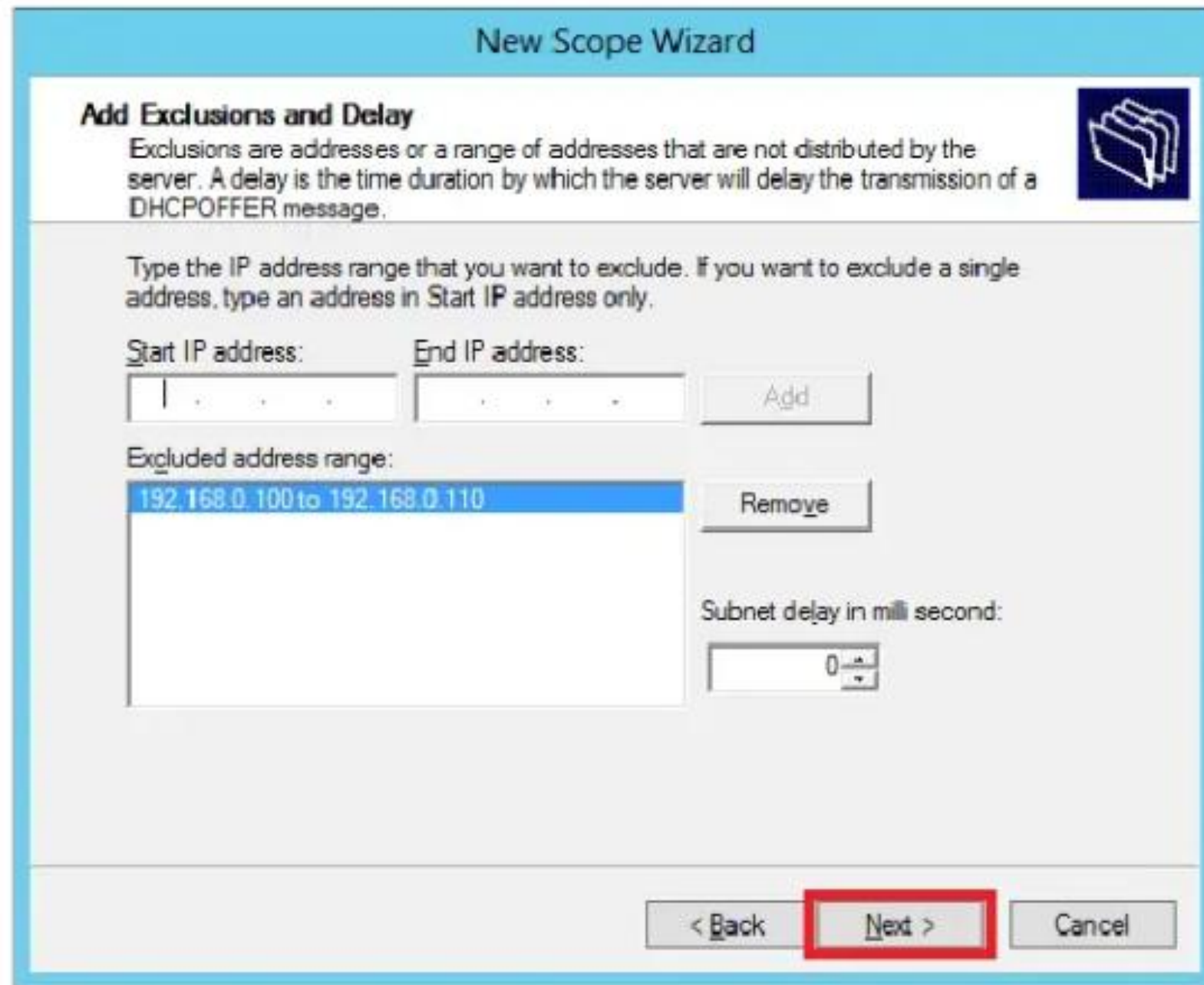
Configuration settings that propagate to DHCP Client

Length: 24
Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel



Step 8 - Enter your IP range in the exclusion list, if you have devices on the network that require static IP address and also ensure that the excluded range falls with the Start and End range earlier specified, then → click Next



New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

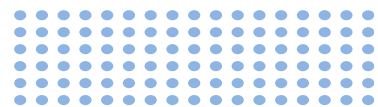
Start IP address: End IP address:

Excluded address range:

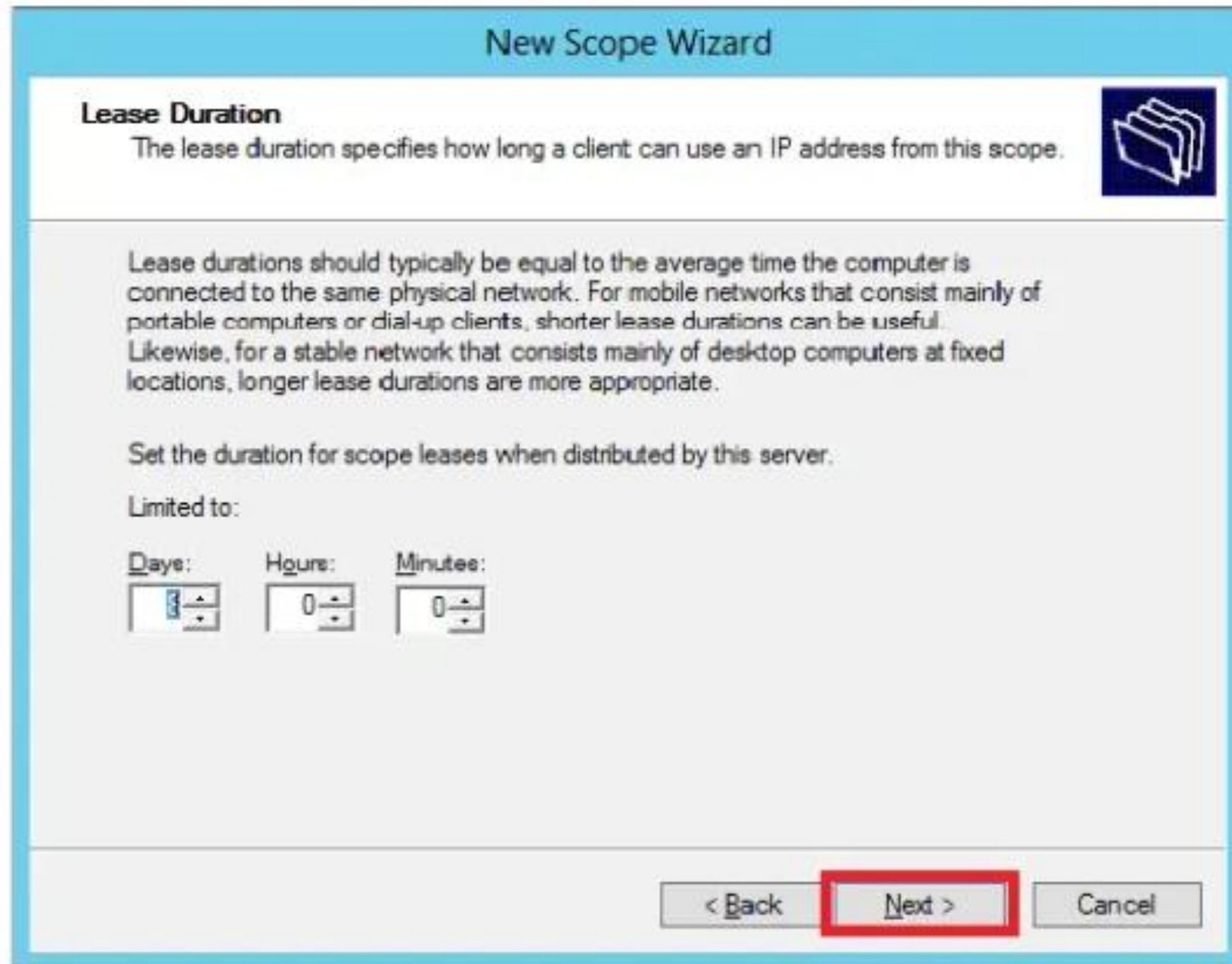
192.168.0.100 to 192.168.0.110	<input type="button" value="Remove"/>
--------------------------------	---------------------------------------

Subnet delay in milliseconds:

< Back **Next >** Cancel



Step 9 - Enter the desired lease duration for the assigned IP's or leave as default → then click Next



New Scope Wizard

Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

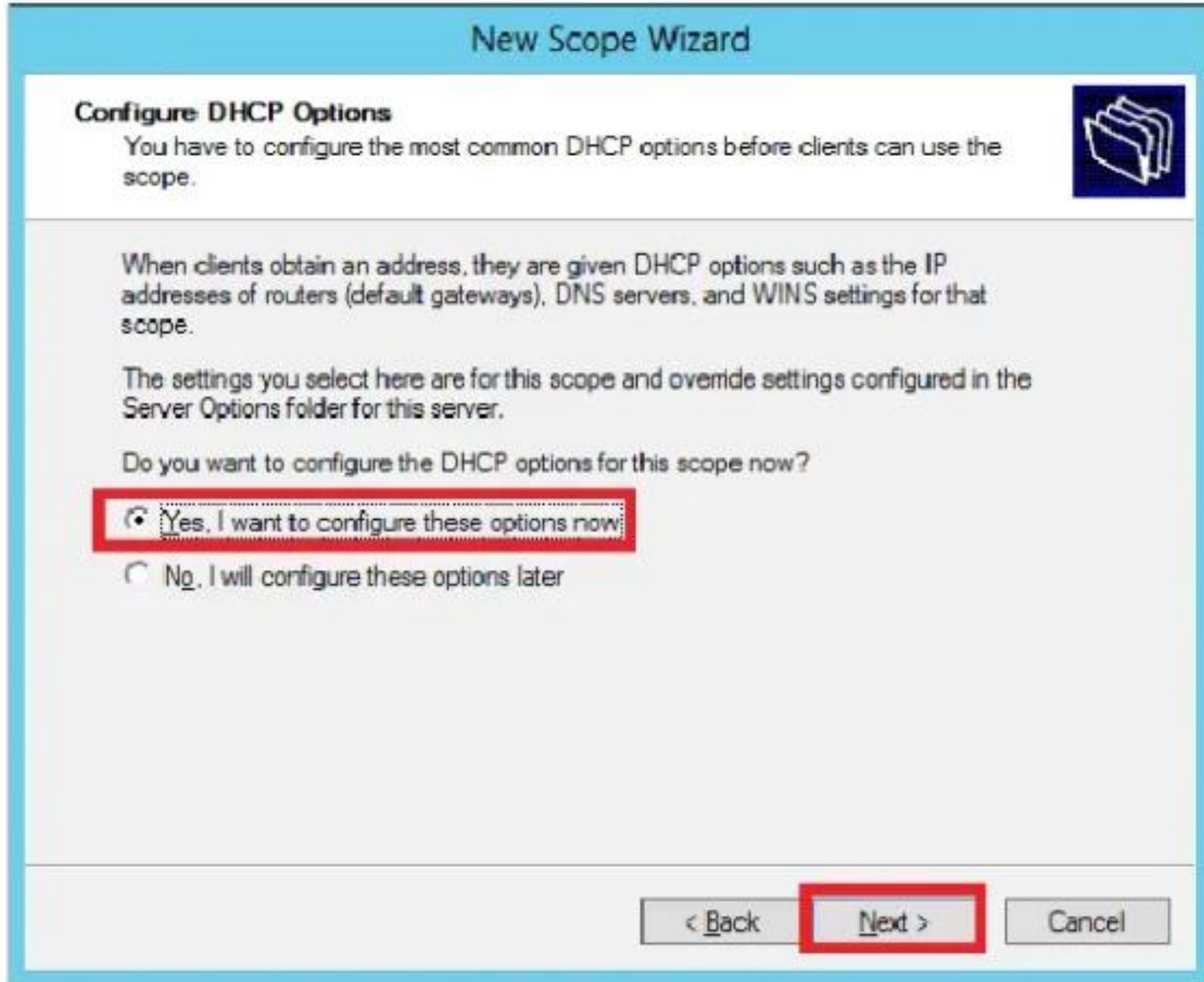
Limited to:

Days:	Hours:	Minutes:
3	0	0

< Back **Next >** Cancel



Step 10 - Select → Yes, I want to configure these option now to configure the DHCP options for the new scope → then click on Next



The image shows a screenshot of the 'New Scope Wizard' window, specifically the 'Configure DHCP Options' step. The window has a light blue title bar and a white background. The title 'New Scope Wizard' is in the top left. Below it, the section 'Configure DHCP Options' is highlighted in blue. The text inside says: 'You have to configure the most common DHCP options before clients can use the scope.' followed by a folder icon. Below this, there is explanatory text: 'When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.' and 'The settings you select here are for this scope and override settings configured in the Server Options folder for this server.' The main question is 'Do you want to configure the DHCP options for this scope now?'. There are two radio button options: 'Yes, I want to configure these options now' (which is selected and highlighted with a red rectangle) and 'No, I will configure these options later'. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a red rectangle), and 'Cancel'.

New Scope Wizard

Configure DHCP Options
You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

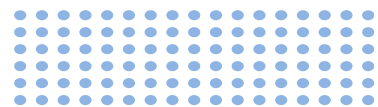
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

☒ Yes, I want to configure these options now

☐ No, I will configure these options later

< Back **Next >** Cancel



Step 11 - Enter the default gateway which is the IP of your Router → Then click Next



The image shows a screenshot of the 'New Scope Wizard' window, specifically the 'Router (Default Gateway)' step. The window has a blue title bar and a light blue header. Below the header, there is a section titled 'Router (Default Gateway)' with a folder icon. The text below this section says 'You can specify the routers, or default gateways, to be distributed by this scope.' Below this, there is a text box labeled 'IP address:' with a small input field containing '192.168.0.1'. To the right of the input field are four buttons: 'Add', 'Remove', 'Up', and 'Down'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red rectangle.

New Scope Wizard

Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

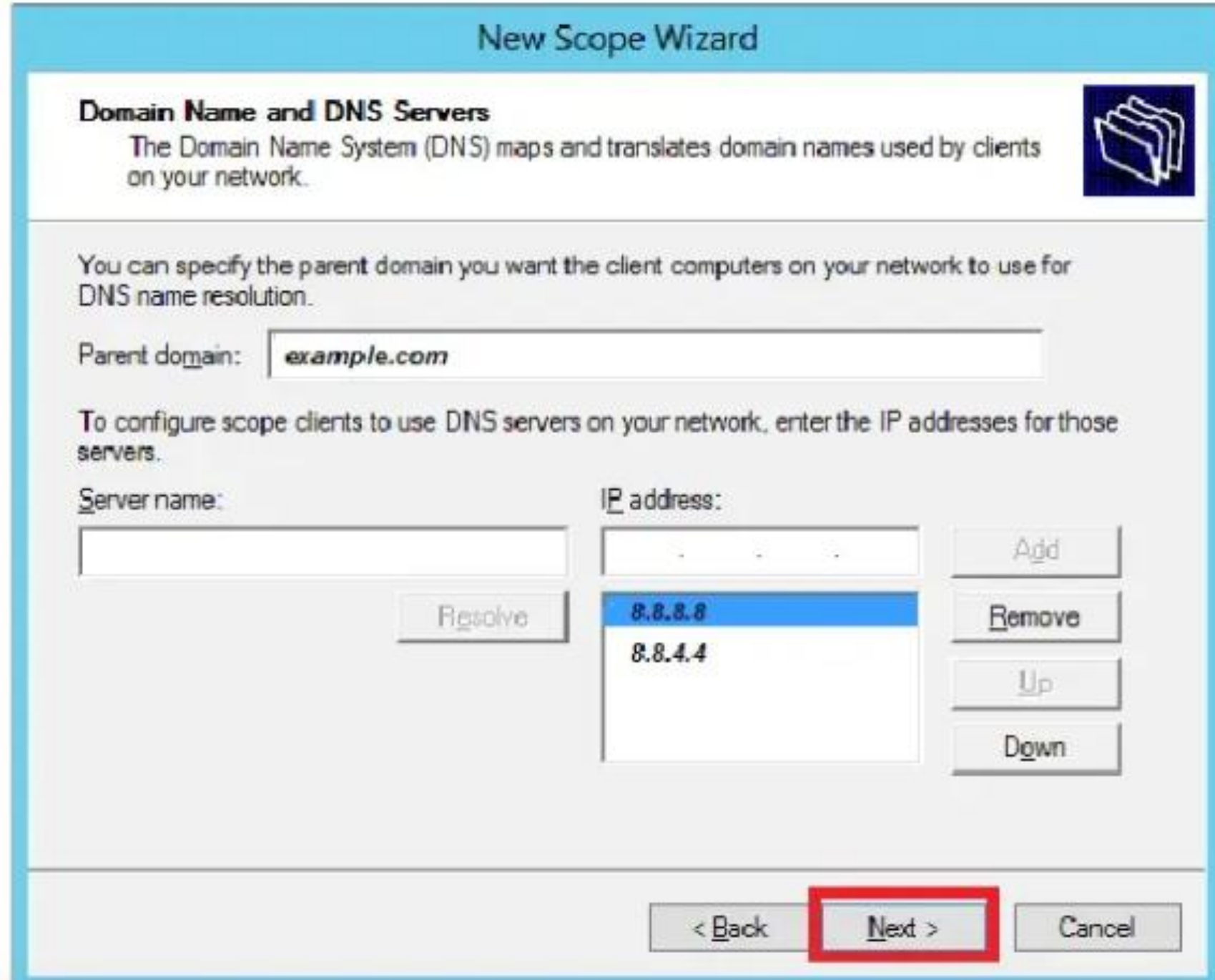
192.168.0.1

Add
Remove
Up
Down

< Back **Next >** Cancel



Step 12- Add DNS IP → click Next (we can put Google DNS or if it is a Domain environment you can put the DC IP there) then click → Next



New Scope Wizard

Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

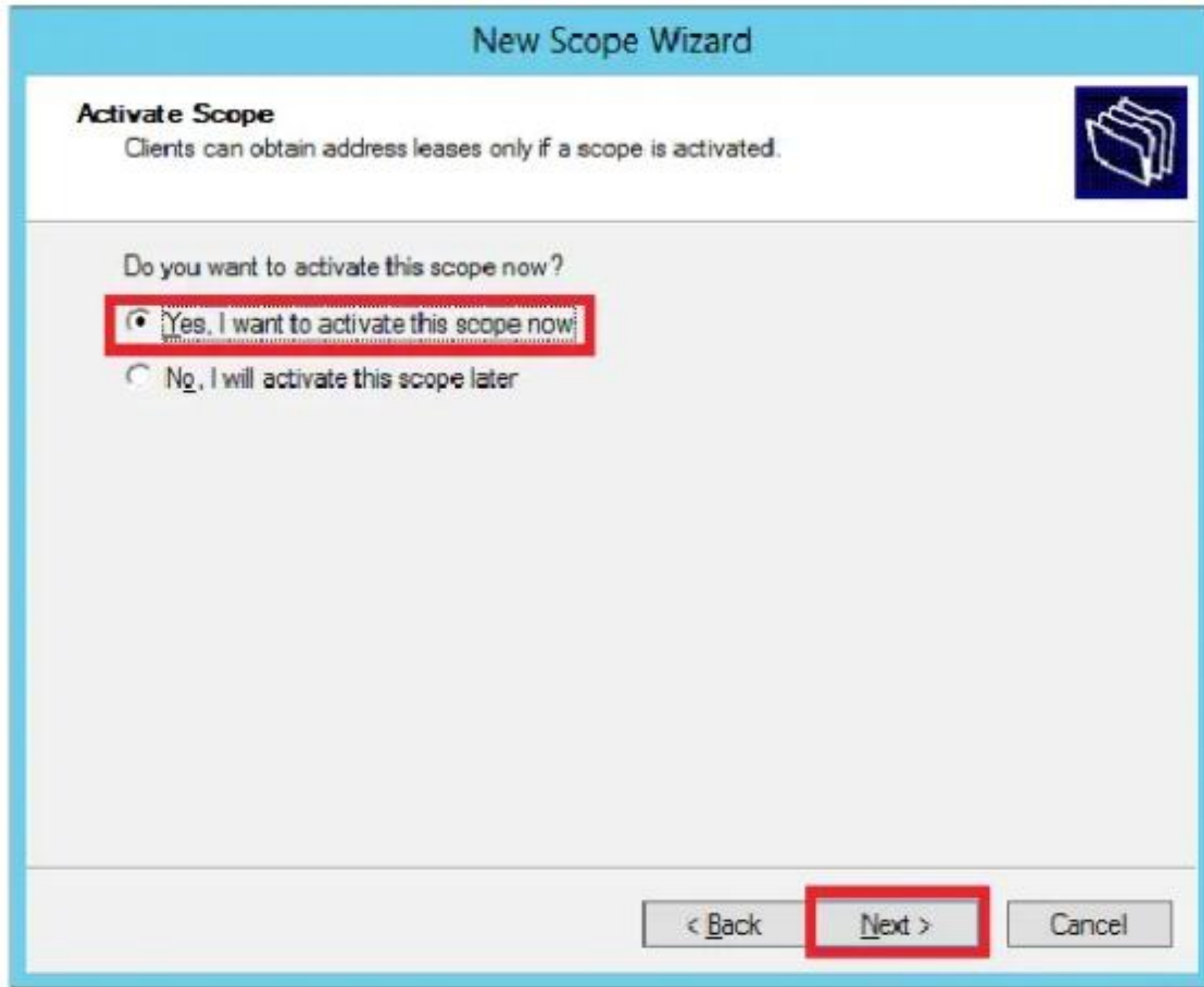
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:	
<input type="text"/>	<input type="text" value="."/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>	<input type="text" value="8.8.8.8"/>	<input type="button" value="Remove"/>
	<input type="text" value="8.8.4.4"/>	<input type="button" value="Up"/>
		<input type="button" value="Down"/>

< Back **Next >** Cancel



Step 13 - select "Yes, I want to activate this scope now" option to activate the scope immediately and then click → Next



New Scope Wizard

Activate Scope
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

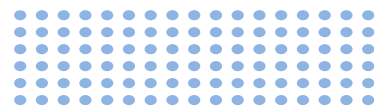
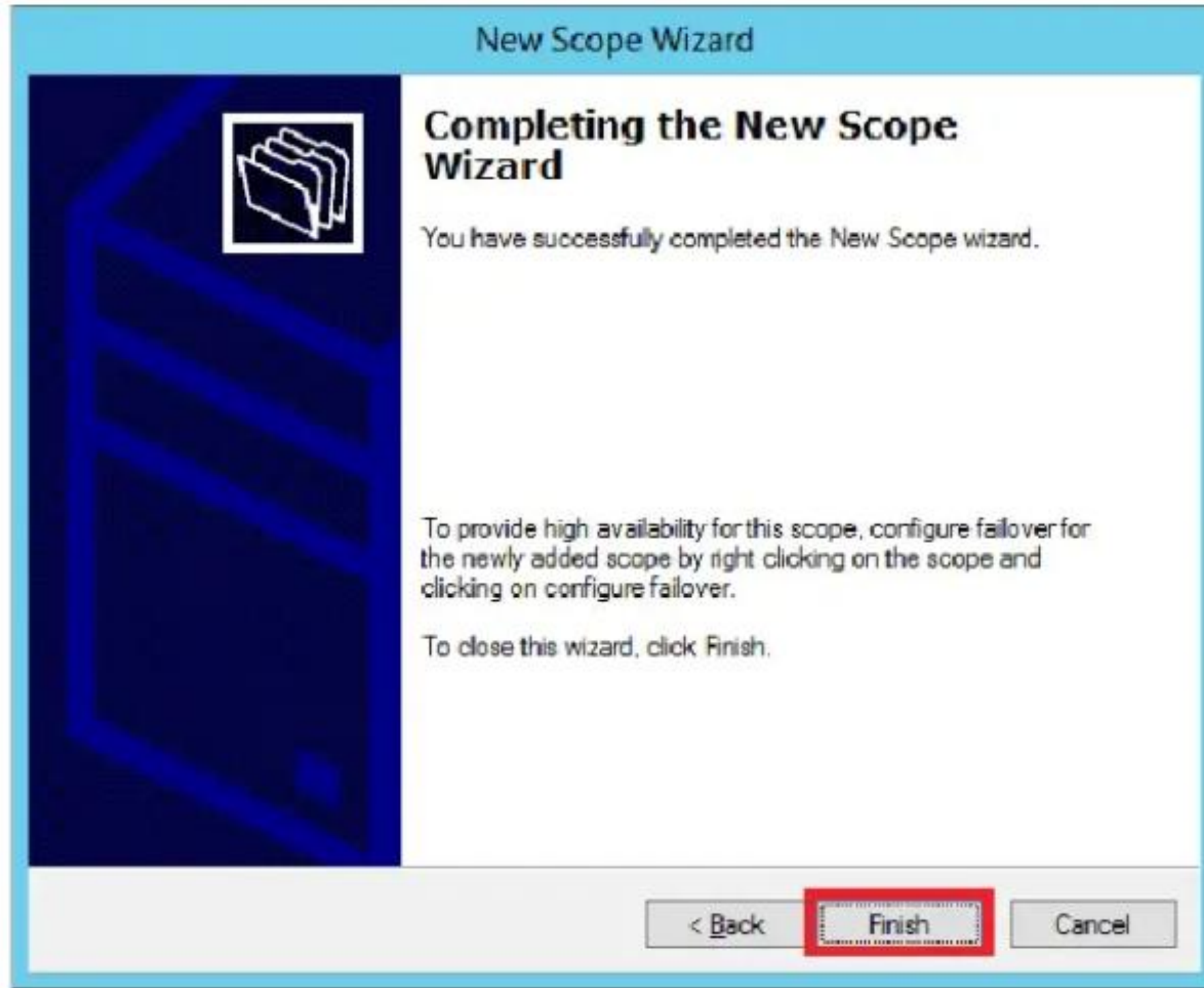
☒ Yes, I want to activate this scope now

☐ No, I will activate this scope later

< Back **Next >** Cancel



Step 14 - Click finish





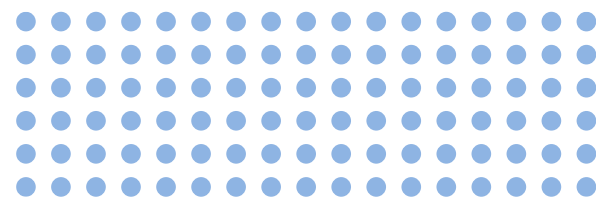
Introduction of Hyenae tool

Hyenae

Hyenae is a highly flexible platform independent network packet generator. It allows you to reproduce several MITM, DoS and DDoS attack scenarios, comes with a clusterable remote daemon and an interactive attack assistant.

Hyenae is a free software published in other list of programs, part of System Utilities.

It is available in English and is compatible with the different operating systems, such as Linux and others.



Installation step for Hyenae in Windows System

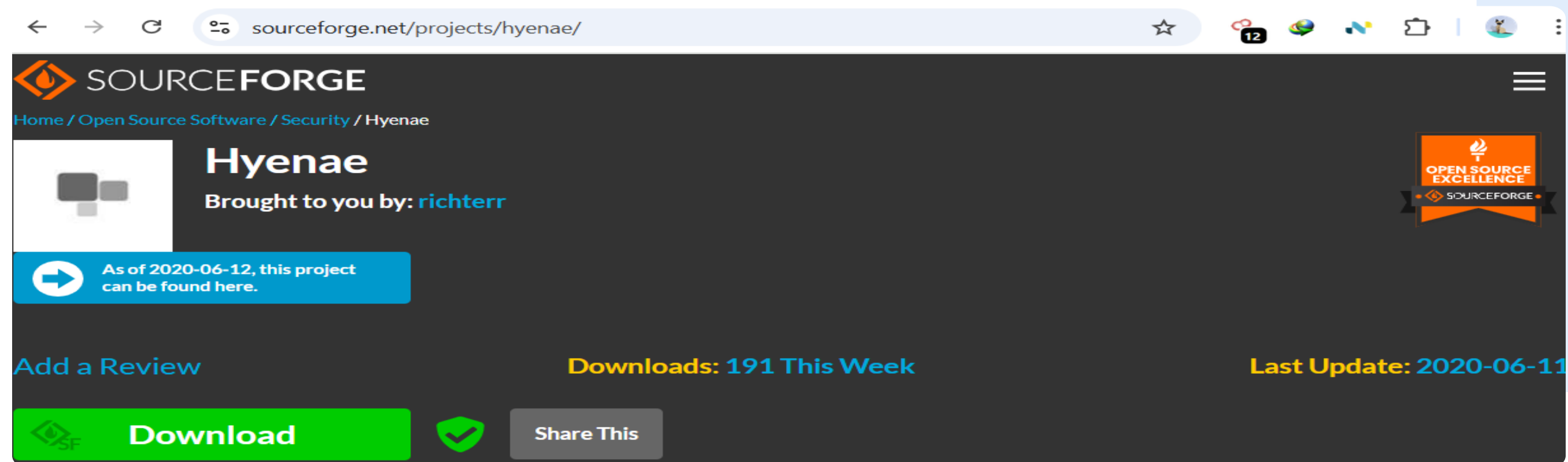


As a versatile network packet generator that supports various attack simulations, including DHCP-related scenarios. To install Hyenae on a Windows system, follow the steps below:

1. Download Hyenae:

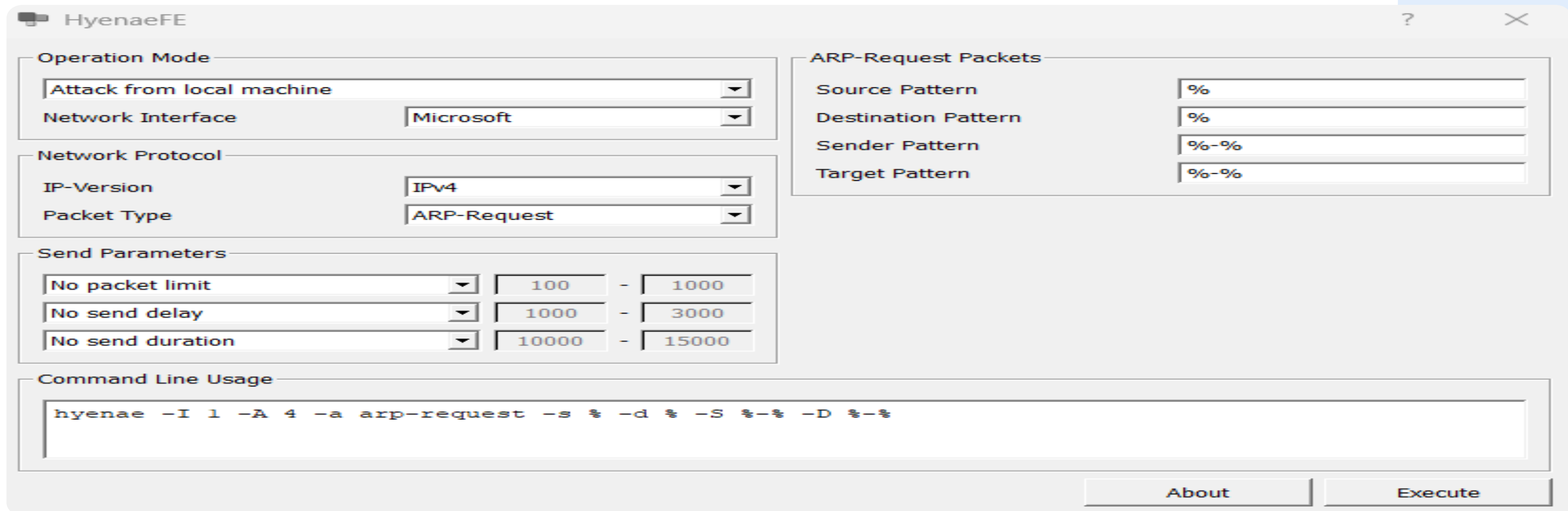
- Visit the official SourceForge page to download the latest Windows version of Hyenae:

<https://sourceforge.net/projects/hyenae/>



2. Install Hyenae:

- Locate the downloaded Hyenae executable file .
- Double-click the file to run the installer.
- Follow the installation prompts:
 - Choose the components to install.
 - Choose the destination folder for installation.
 - Confirm and complete the installation process.



The screenshot shows the HyenaeFE application window with the following settings:

- Operation Mode:** Attack from local machine
- Network Interface:** Microsoft
- Network Protocol:**
 - IP-Version: IPv4
 - Packet Type: ARP-Request
- Send Parameters:**
 - No packet limit: 100 - 1000
 - No send delay: 1000 - 3000
 - No send duration: 10000 - 15000
- ARP-Request Packets:**
 - Source Pattern: %
 - Destination Pattern: %
 - Sender Pattern: %-%
 - Target Pattern: %-%
- Command Line Usage:**

```
hyenae -I 1 -A 4 -a arp-request -s % -d % -S %-% -D %-%
```

Buttons at the bottom: About, Execute

DHCP Attack using Hyenae

In this agenda I will explain how to perform a DHCP starvation attack from a Windows machine (host) targeting a Windows Server VM running as a DHCP server.

1

Before starting testing with Hyenae, make sure your primary Windows can communicate with your Windows Server:

```
C:\Windows\System32>ping 192.168.174.220
```

```
Pinging 192.168.174.220 with 32 bytes of data:
```

```
Reply from 192.168.174.220: bytes=32 time=4ms TTL=128
```

```
Reply from 192.168.174.220: bytes=32 time=6ms TTL=128
```

```
Reply from 192.168.174.220: bytes=32 time=3ms TTL=128
```

```
Reply from 192.168.174.220: bytes=32 time=2ms TTL=128
```

```
Ping statistics for 192.168.174.220:
```

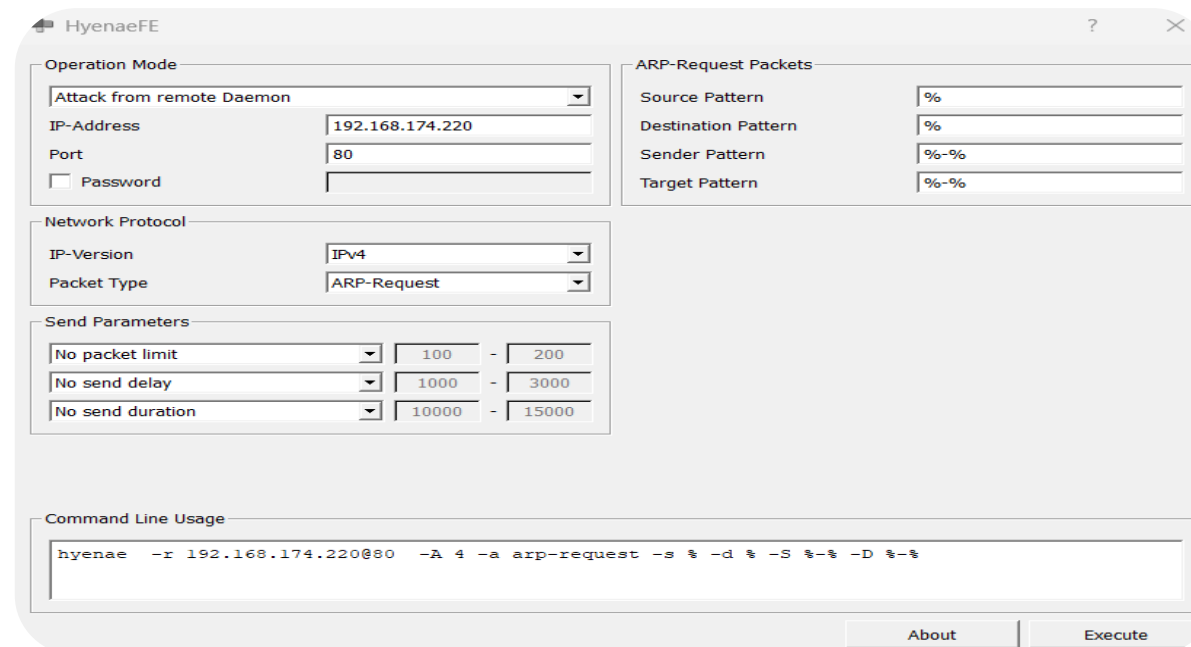
```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 2ms, Maximum = 6ms, Average = 3ms
```

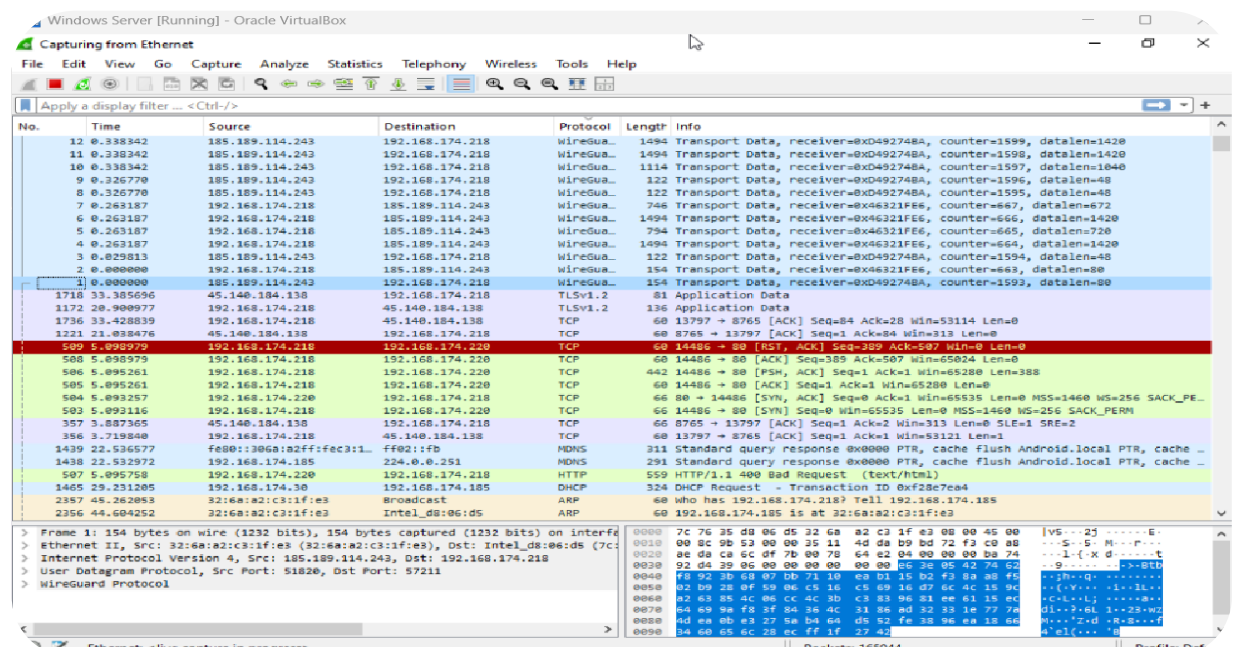
2

start training with Hyenae by sending malicious packets to Windows Server.



3

Wireshark on Windows Server to view packets being sent



View packets being sent

HyenaeFE

Operation Mode

Attack from remote Daemon

IP-Address192.168.174.220

Port80

☐ Password

Network Protocol

IP-VersionIPv4

Packet TypeARP-Request

Send Parameters

No packet limit100 - 200

No send delay1000 - 3000

No send duration10000 - 15000

Command Line Usage

hyenae -r 192.168.174.220@80 -A 4 -a arp-request -s % -d % -S %-% -D %-%
* Initializing
* Launching remote attack

ARP-Request Packets

Source Pattern%

Destination Pattern%

Sender Pattern%-%

Target Pattern%-%

About

Execute

The image show an attempted remote ARP attack using Hyenae, where:

Operation Mode:

The attack via remote Daemon (Hyenae background service) was selected.

The target is Windows Server with IP 192.168.174.220, with port 80.

Protocol Configuration:

Protocol: IPv4 with ARP-Request type packets (used for spoofing or ARP poisoning attacks).

Start training with Hyenae by sending malicious packets to Windows Server.

No.	Time	Source	Destination	Protocol	Length	Info
1407	26.919171	192.168.174.218	154.47.31.167	TCP	262	[TCP Retransmission] 5953 → 8765 [PSH, ACK] Seq=1041 Ack=1 Win=53008 Len=...
1408	27.134064	154.47.31.167	192.168.174.218	TCP	60	8765 → 5953 [ACK] Seq=1 Ack=1249 Win=650 Len=0
1726	32.032119	154.47.31.167	192.168.174.218	TCP	60	8765 → 5953 [ACK] Seq=1 Ack=1457 Win=652 Len=0
2006	36.971251	154.47.31.167	192.168.174.218	TCP	60	8765 → 5953 [ACK] Seq=1 Ack=1665 Win=654 Len=0
2007	37.087789	34.149.100.209	192.168.174.30	TCP	66	443 → 47616 [ACK] Seq=1 Ack=47 Win=1050 Len=0 TSval=3301298226 TSecr=2283...
2009	37.129843	192.168.174.30	34.149.100.209	TCP	66	47616 → 443 [ACK] Seq=47 Ack=47 Win=631 Len=0 TSval=2283144032 TSecr=3301...
2116	42.022355	154.47.31.167	192.168.174.218	TCP	60	8765 → 5953 [ACK] Seq=1 Ack=1873 Win=656 Len=0
2142	47.188814	154.47.31.167	192.168.174.218	TCP	60	8765 → 5953 [ACK] Seq=1 Ack=2081 Win=658 Len=0
2417	52.267907	154.47.31.167	192.168.174.218	TCP	60	8765 → 5953 [ACK] Seq=1 Ack=2289 Win=660 Len=0
2764	57.328051	154.47.31.167	192.168.174.218	TCP	60	8765 → 5953 [ACK] Seq=1 Ack=2497 Win=662 Len=0
2839	62.388357	154.47.31.167	192.168.174.218	TCP	60	8765 → 5953 [ACK] Seq=1 Ack=2705 Win=664 Len=0
2990	67.375091	154.47.31.167	192.168.174.218	TCP	60	8765 → 5953 [ACK] Seq=1 Ack=2913 Win=667 Len=0
3310	72.461529	154.47.31.167	192.168.174.218	TCP	60	8765 → 5953 [ACK] Seq=1 Ack=3121 Win=669 Len=0
3338	73.147010	192.168.174.218	192.168.174.220	TCP	66	6927 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
3339	73.147289	192.168.174.220	192.168.174.218	TCP	66	80 → 6927 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
3340	73.148015	192.168.174.218	192.168.174.220	TCP	60	6927 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
3341	73.148015	192.168.174.218	192.168.174.220	TCP	442	6927 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=388
3343	73.149493	192.168.174.218	192.168.174.220	TCP	60	6927 → 80 [ACK] Seq=389 Ack=507 Win=65024 Len=0
3344	73.149493	192.168.174.218	192.168.174.220	TCP	60	6927 → 80 [RST, ACK] Seq=389 Ack=507 Win=0 Len=0

<p>> Frame 3344: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface</p> <p>> Ethernet II, Src: Intel_d8:06:d5 (7c:76:35:d8:06:d5), Dst: PCSSystemtec_e6:dd:</p> <p>> Internet Protocol Version 4, Src: 192.168.174.218, Dst: 192.168.174.220</p> <p>> Transmission Control Protocol, Src Port: 6927, Dst Port: 80, Seq: 389, Ack: 507</p> <p>Source Port: 6927</p> <p>Destination Port: 80</p> <p>[Stream index: 2]</p> <p>[Stream Packet Number: 7]</p> <p>> [Conversation completeness: Complete, WITH_DATA (63)]</p> <p>[TCP Segment Len: 0]</p> <p>Sequence Number: 389 (relative sequence number)</p> <p>Sequence Number (raw): 3997536203</p> <p>[Next Sequence Number: 389 (relative sequence number)]</p> <p>Acknowledgment Number: 507 (relative ack number)</p> <p>Acknowledgment number (raw): 141691336</p> <p>0101 = Header Length: 20 bytes (5)</p> <p>> Flags: 0x014 (RST, ACK)</p> <p>Window: 0</p>	<pre> 0000 08 00 27 e6 dd ea 7c 76 35 d8 06 d5 08 00 45 00 ..^... V 5.....E. 0010 00 28 bd df 40 00 00 06 5d e8 c0 a8 ae da c0 a8 -(..@...]-..... 0020 ae dc 1b 0f 00 50 ee 45 8f cb 08 72 09 c8 50 14 P.E...P..P. 0030 00 00 25 1e 00 00 00 00 00 00 00 00 00 00 00 ..%...... </pre>
--	---

Ethernet: <live capture in progress> Packets: 74985 Profile: Default

The screenshot image show a complete TCP handshake between IP 192.168.174.218 (primary host) and 192.168.174.220 (Windows server on port 80), starting with a SYN from the primary host (port 6927), followed by a SYN-ACK from the server and an acknowledgement ACK (packets 3338-3340). After establishing the connection, the primary host send data (388-byte PSH,ACK in packet 3341) and ends with an acknowledgement ACK (3343) and a possible abnormal termination (LSI,ACK in packet 3344, which would normally be FIN,ACK to close the connection properly). The pattern indicates a normal HTTP communication, but with an abnormal termination.

Conclusion

This project aimed to demonstrate a DHCP starvation attack using the Hyenae tool, simulating a real-world scenario where an attacker exhausts the available IP addresses on a DHCP server, causing disruptions to network operations.

The Hyenae tool was not effective on Windows 11 as a primary system, which is believed to have been better on Kali Linux.

In summary, this project highlighted the need to protect critical network services, such as DHCP, from malicious exploits, reinforcing the importance of cybersecurity awareness and best practices.





References

- ❑ dhcp-protocol. (2025). Retrieved from portnox.com: <https://www.portnox.com/cybersecurity-101/dhcp-protocol/>
- ❑ hyenae. (2020, 06 24). Retrieved from github.com: <https://github.com/r-richter/hyenae>
- ❑ Protocolo DHCP. (2024, 11 02). Retrieved from learn.microsoft.com: <https://learn.microsoft.com/pt-br/windows-server/networking/technologies/dhcp/dhcp-top>





**THANK
YOU!**



wilsoncanetekamacupa@gmail.com

